

## Annex A Financial Control Framework

Financial Control Framework		
Risk	Description	Control
Fraudulent use of a Defence credit card	Card holders who have left Defence do not advise the Corporate Card Support Centre (CCSC) that tier cards require cancelling.	Conducted monthly by the Corporate Card Support Centre (CCSC) identifies active cards where the card holder is no longer on PMKeys. Identified cards are then cancelled.
Unauthorised and fraudulent use of Defence credit cards.	Opportunity for all Defence credit card holders to misuse their Defence Credit Card	Inspector Generals department provide a targeted fraud detection program.
Unauthorised use of a Defence credit card	Unauthorised use of Defence credit card to purchase items for personnel use.	2 person approval process where the CMS supervisor is required to check to ensure that acquittals have only occurred for pre approved business/travel purposes only
DPC Cash access requests	Card holders requesting cash access on DPC's	All requests to access cash through the DPC require group CFO approval and FASRA sign off. There is a register of all requests and a QA which is conducted 6 monthly where card holders are asked if cash access is still required.
Request to increase limit on defence Credit card.	Card holder requests an increase in the credit limit for their card.	All requests to increase the credit limit on a Defence credit card need to be accompanied with a business case and supervisor approval. QA 2.1.10 run 12 monthly identifies high limit cards and the card holders are contacted and requested if the high limit is still required and are required to provide justification.
Unauthorised withdrawal of large amounts of money using DTC.	Card holders ability to withdraw large amounts of money form Travelex without approval	Cash withdrawals over \$10,000 require the CCSC to be informed and provided with prior approval from their supervisor. The vendor will contact the CCSC and ask for approval prior to dispensing the money.

Financial Control Framework		
Risk	Description	Control
Unauthorised person requesting a Defence credit card.	Anyone who has DRN access has the ability to apply for a Defence credit card	QA conducted by CCSC on receipt of applications to ensure that the applicant is a Defence official. Checks include PMKeys and personnel data.
Unauthorised opening of a Cabcharge account	Any person who has a Defence email can open a Cabcharge account and charge the account to Defence	None
Fraudulent use of Defence Cabcharge e-tickets	Lack of control and monitoring of Cabcharge e-tickets once they have been issued.	Unknown. Units may have local rules regarding the issuing and monitoring and issuing of Cabcharge e-tickets
Distribution of Cabcharge e-tickets to Defence contractors and consultants	Lack of knowledge that Defence contractors and consultants are not entitled to be issued with Cabcharge e-tickets as they are not considered Defence officials	Unknown. Units may have local rules regarding the issuing and monitoring and issuing of Cabcharge e-tickets
Incorrect use of Cabcharge e-tickets	Cabcharge e-tickets are being issued to defence members instead of the member being directed to use DTC.	Customer Service Centres (CSC) issue Cabcharge e-tickets strictly in accordance with the type of travel.

**FCF before audit**

## Annex B Financial Control Framework Current

Control Activities	Role Responsible	Purpose
<p>Card Application Processing System (CAPS) initiates automatic cancellation of credit card based on matching of card holders with daily feed from PMKeys employee data.</p> <p>Annual QA identifies purchase cards holders with limit over 250,000 to confirm if the high limit is still required</p> <p>DFAC conducts monthly review of 100% credit card transactions for pre-defined high risk merchant categories and any unusual spending patterns are investigated.</p> <p>Expenses are monitored by cost centre managers.</p>	<p>CFOG – DFAC</p> <p>CFOG</p> <p>CFOG – DFAC</p> <p>ALL</p>	<p>To ascertain fraudulent use of a Defence credit card.</p> <ul style="list-style-type: none"> <li>Identify card holders who have left Defence and whereby the Corporate Card Support Centre has not been identified to cancel card.</li> <li>Collusion between CMS supervisor and cardholder</li> <li>Card holders can dispute transactions to hide fraud</li> </ul>
<p>Audit and Fraud Control Division conducts a targeted fraud detection program which includes credit cards.</p> <p>DFAC conducts monthly review of 100% credit card transactions for pre-defined high risk merchant categories and any unusual spending patterns are investigated.</p> <p>Any credit card transactions not supported by adequate explanation are referred to Director Fraud Control</p> <p>CMS Supervisors are determined by the Group CFO or their delegate.</p> <p>Credit cards not activated within 90 days are cancelled.</p> <p>All physical credit cards are subject to unique pin codes.</p> <p>Two merchant codes considered inappropriate have been blocked.</p> <p>Two person approval process: CMS prevents cardholders to accept their own transaction</p>	<p>DAFD</p> <p>CFOG- DFAC</p> <p>ALL</p> <p>GROUP CFO'S</p> <p>CFOG-DFO</p> <p>CFOG-DFO</p> <p>CFOG-DFO</p> <p>CFOG- DFO</p>	<p>To identify unauthorised and or fraudulent use of Defence Credit Card, as there is the opportunity for all Defence Credit card holders or outsiders to misuse their Defence Credit Card.</p>
<p>Two person approval process: All Credit Card transactions are validated (including acquittals of only pre-approved expenses) by a CMS Supervisor.</p> <p>System alert has been implement to notify incoming and outgoing supervisors when change in supervisor occurs.</p>	<p>ALL</p> <p>CFOG-DFO &amp; Supervisors</p>	<p>To identify unauthorised use of Defence credit card to purchase items for personnel use.</p>

Control Activities	Role Responsible	Purpose
<p>All requests to access cash through the DPC require Group CFO approval and FASRA sign off. A register of all requests is maintained and a QA is conducted annually where card holders are asked if cash access is still required.</p> <p>DPC cash withdrawals are reviewed monthly and any withdrawal without FASRA signoff are forwarded to Group CFO</p> <p>\$0 default cash transfer limit is set for all <b>new</b> Purchasing Cards and any change to the default cash transfer limit for Purchasing Card requires approval of Group CFOs.</p> <p>Existing DPC cards will have \$0 default cash withdrawal during the move to ANZ unless Group CFO approval is provided.</p>	<p>CFOG-DFO</p> <p>CFOG-DFAC</p> <p>CFO – DFO</p> <p>CFO- DFO</p>	<p>To identify unauthorised withdrawal of money using DPC, as there is the opportunity for card holders to withdraw cash from DPC</p>

## **Annex C Fuel Control Framework**

### **Fuel Card Controls**

1. The following controls were in prior to the audit:

#### **V05S07C01B - USE OF DEFENCE FUEL CARDS MANAGED BY THE JOINT FUELS AND LUBRICANTS AGENCY**

##### **INTRODUCTION**

2. The purpose of this document is to define the policy for the use and management of Defence fuel cards administered by the Joint Fuels and Lubricants Agency (JFLA) within Defence and its associated agencies, and define the roles and responsibilities of key personnel. JFLA have overarching responsibility for implementing and maintaining a framework that supports good governance, and identifies and mitigates Defence fuel card misuse or fraud.
3. There are two Defence fuel card types; Generic fuel cards which are not assigned to a specific vehicle/aircraft; and Vehicle Specific fuel cards which are specifically assigned to a vehicle/aircraft. Defence fuel card holdings comprise Ground and Aviation fuel cards.
4. There are two Defence fuel card categories; Commercial cards which can be used at specific commercial service stations and Petrol, Oil and Lubricants (POL) sites and Defence on-base cards which can only be used at Defence POL installations fitted with FUELSCAN.
5. Defence ground fuel card holdings and transactions are recorded and managed through the Australian Defence Organisation Fuel Card Management System (ADOFMS). In the case of Aviation Fuel Cards, only fuel card holdings are recorded and managed through the ADOFMS.
6. For the purpose of this instruction all references to Defence fuel cards are to read as JFLA Administered Fuel Cards; and Defence Fuel Card Policy is to read as the Policy for the Use and Administration of Defence Fuel Cards Managed by the JFLA.

##### **SCOPE**

7. This policy applies to all organisations and personnel involved in Defence Fuel Card use and management processes administered

by JFLA, including authorised Australian Defence personnel and Defence contractors. This policy does not apply to the use of fuel cards provided as part of a leased or hire vehicle contract or those associated with Defence's Executive Vehicle Scheme

## **POLICY STATEMENT**

8. All fuel card users, ADOFMS delegates, Commanding Officers (CO) and JFLA staff are responsible for ensuring the proper control and use of Defence fuel cards. This document defines JFLA's oversight, responsibilities and the assurance activities for monitoring compliance, and the Business Rules and Audit and Review Guidelines that all organisations and personnel involved in any aspects of Defence fuel card use and management must adhere to; this includes authorised Australian Defence personnel and Defence contractors who are responsible for managing fuel cards on behalf of a nominated ADO or group of units.
9. The business rules contained in this policy define the parameters for the use and management of Defence fuel cards; the Audit and Review Guidelines assist all personnel and organisations to perform audit and review procedures to comply with the business rules set by this policy, which has been agreed to by the services.
10. JFLA is committed to maintaining a governance framework that reflects the requirements set out in key regulations and policies that address the treatment of Defence fuel card misuse or fraud, namely:
  - a. Financial Management and Accountability Act 1997 - Section 60 Misuse of Commonwealth Credit Cards
  - b. APS Code of Conduct
  - c. Defence Force Discipline Act (1982)
  - d. Defence Instructions (General) ADMIN 45-2 The Reporting and Management of Notifiable Incidents
  - e. V05S07C01B2 Defence Fuel Card Fraud Control Plan
  - f. Commonwealth Procurement Guidelines
  - g. Defence Procurement Policy Manual
  - h. Defence Chief Executive Instructions (CEI) 2.1 Procurement and 2.3 Corporate Cards.
  - i. DMO Chief Executive Instructions (CEI) 2.1 - Procurement and 2.3 Corporate Cards

## **DEFINITIONS**

11. The following definitions apply to this instruction:

- a. **ADOFMS Delegate.** A person who has been given the authority to manage fuel cards within their unit. Each unit is to have a maximum of two delegates. An authorising officer and an alternative authorising officer. ADOFMS delegates can manage multiple units if required.
- b. **Unit.** A Defence organisation which is managed by a Commanding Officer or Officer Commanding.
- c. **Defence Fuel Card Systems Administrator.** Transponder Technologies (TT) is a sub-contractor engaged to provide and maintain the ADOFMS application, including both hardware and software. The ADOFMS application is a component of an application called FuelsManager, which is managed by a company called Varec Inc. TT are contracted to Defence through Varec Inc. The FuelsManager application is provided to Defence through a contract managed by the Logistics Information Systems Branch.
- d. **Vehicle Specific fuel card.** A fuel card that is specifically assigned to a vehicle, aircraft or vessel. Should only be used against the equipment for which it is intended.
- e. **Generic fuel card.** A fuel card that is not assigned to a specific vehicle, aircraft or vessel. Can be used for equipment such as plant, generators or loan pool vehicles.
- f. **Approved Unit.** A unit that has been excluded from having their fuel cards cancelled as a consequence of the cards not being used within 12 months. An approved unit is identified as those involved with immediate response activities. JFLA is the authority and will maintain a list of Approved Units.

## **ROLES AND RESPONSIBILITIES**

12. The following section describes:

- a. JFLA responsibilities
- b. Business Rules and
- c. Audit and Review Guidelines.

- d. [V05S07C01B1](#) provides guidance on the roles and responsibilities of the key personnel involved in Defence Fuel Card usage and management.

### **JFLA Responsibilities**

13. JFLA is responsible for managing the Defence fuel card system and it has an overarching responsibility to implement and maintain a framework that supports good governance. JFLA oversight and assurance activities have been designed to monitor compliance, and their responsibilities include:
14. Setting and updating policy and guidelines in relation to fuel card usage and management;
15. Developing and monitoring execution of an annual assurance program to confirm controls are effective and are operating as designed;
16. Endorsing the results of assurance activities and ensuring remediation action is implemented where required;
17. Regularly communicating follow up action taken to remediate problems in relation to the Australian Defence Organisation Fuel Card Management System (ADOFMS);
18. Performing audit and review procedures: and
19. Validating supplier invoices and arranging payment.

### **JFLA Annual Assurance Program**

20. To ensure an appropriate level of scrutiny and accountability is being applied to the use and management of Defence fuel cards, JFLA will develop and oversee an annual assurance program to confirm that roles and responsibilities are being adhered to, and that key controls to identify and mitigate opportunities for fraud are in place and operating effectively. The annual assurance program is developed with consideration to the Fuel Card Risk Control and Analysis Results.
21. In preparing the assurance plan JFLA will:
  - a. focus on testing controls mitigating inherent fraud risks rated high to very high;



- b. focus on fraud risk issues identified/reported by units that are likely to be prevalent throughout other Defence units
  - c. align where possible with other site visit audits being conducted within Defence
  - d. select a sample of units to perform control testing to assist JFLA to confirm compliance with business rules set within this policy. Selection of which units to include should be guided by an assessment of where the greatest potential risk for fraud exists amongst the fuel card user community. For example:
    1. units with a high volume of transactions per month to confirm transactions are being appropriately validated;
    2. units with a high percentage of generic cards to confirm fuel card type is valid and appropriate; and
    3. metropolitan units with a high number of vehicle specific fuel cards to verify the number of vehicle specific cards are kept to a minimum.
  - e. select a random sample of units to perform a standard audit test program throughout the year.
22. JFLA may seek the assistance of MAB, the DFCF or an external consultant to provide this assurance activity.

### **JFLA Audit and Review Guidelines**

23. The following exception reports shall be generated and appropriate action taken by JFLA on a monthly basis:

	<b>Exception Reports</b>	<b>Action To Take</b>
1	Active fuel cards not used for 12 months (with the exception of Approved Units, such as units involved with immediate response activities)	Forward report to Varec for cancellation of fuel card in ADOFMS and notify ADOFMS delegate that the fuel card has been cancelled and should be physically destroyed.
	Generated by JFLA	Action taken by JFLA and Varec.
2	Active fuel cards not verified for two months.	Forward report to Varec for cancellation of fuel card in ADOFMS and notify ADOFMS delegate that the fuel card has been cancelled and should be physically destroyed.
	Generated by JFLA	

Exception Reports	Action To Take
3 Active fuel cards without a unit.  Generated by JFLA	Action taken by JFLA and Varec. Forward report to Varec for cancellation of fuel card in ADOFMS
5 Cancelled fuel cards with transactions  Generated by JFLA	Action taken by JFLA and Varec Forward report to ADOFMS delegate to resolve with fuel supplier and Defence Fuel Card Systems Administrator
6 Unreconciled transactions  Generated by JFLA	Action taken by JFLA and ADOFMS delegate Send report to ADOFMS delegate to reconcile transactions within the specified time period.
7 Unverified fuel cards with transactions  Generated by JFLA	Action taken by JFLA and ADOFMS delegate Send report to ADOFMS delegate to verify card in ADOFMS and confirm validity of transaction
8 Delegate pairs with more than 500 transactions per average month (per quarter)  Generated by JFLA	Action taken by JFLA and ADOFMS delegate Send report to CO to determine whether ADOFMS delegate has sufficient capacity to appropriately review all transactions within the month, or alternatively create a second unit.
9 Aging Dispute Transaction (remain unresolved for more than 30 days from the date they were disputed)  Generated by JFLA	Action taken by JFLA and Unit CO Forward report to CO to investigate aged dispute transaction with fuel supplier.  Action taken by JFLA and Unit Co

## Payment for POL Supplies

24. With the exception of those transactions related to Aviation Fuel Cards, JFLA shall seek to confirm that delegates have correctly discharged their responsibilities, under the policy by confirming the following:
25. Transaction listings have been provided and loaded into ADOFMS to support the supplier invoice;
26. Transaction listings match the value of the invoice;
27. Transactions have been accepted by the ADOFMS delegate (or as contractually agreed between JFLA and the card product provider); and
28. Mark for attention any disputed investigation that appears unlikely to be resolved prior to the payment due date, so that appropriate and timely follow up takes place.

29. Where ADOFMS delegates have not reconciled transactions in accordance with this policy, JFLA are to immediately notify the relevant delegate, as failure by the delegate to reconcile transactions may lead to late payment of invoices.
30. In accordance with current Commonwealth policy and extant Standing Offer arrangements, JFLA have an obligation to ensure that payment terms and conditions are adhered to. Where inaction by an ADOFMS delegate is likely to cause late payment through no fault of the supplier, then JFLA will be obliged to process the relevant invoice for payment. However, a report of aged unreconciled transactions will be sent to Service Headquarters and will be reported in the JFLA monthly Certificate of Compliance.

### **JFLA Retention and Record Keeping**

31. JFLA is required to retain the following paper and electronic documents to meet administrative needs and for audit purposes, and ensure that they are kept for seven years after the records were prepared or obtained.

Process	Documents to be retained for seven years
Appoint new ADOFMS delegate	Defence Fuel Card System Delegate Registration Form (AE153)
Fuel card entitlement	Business Case approval by CO
Payment of Fuel Suppliers	Fuel Supplier Invoice
	Suppliers transaction listing
Monthly exception reporting	Evidence of review of exception reports as listed below <ul style="list-style-type: none"> <li>○ Active fuel cards not used in 12 months</li> <li>○ Active Fuel cards not verified in two months</li> <li>○ Active Fuel Cards without a unit</li> <li>○ Active specific Fuel Cards without a vehicle</li> <li>○ Inactive Fuel Cards with transactions</li> <li>○ Unreconciled transactions</li> <li>○ Unverified Fuel Cards with transactions</li> <li>○ Delegation pairs with transactions exceeding 500 per average month (per quarter)</li> <li>○ Ageing dispute transactions</li> <li>○ Vehicle specific fuel cards incurring multiple transactions on the same day</li> <li>○ Transactions greater than vehicle capacity</li> <li>○ Fuel card expiring within 2 months</li> </ul>

32. The following business rules must be adhered to by all organisations and personnel involved in any aspects of Defence fuel card use and management processes. Any breach of these rules may result in the cancellation of Defence fuel cards and/or disciplinary action.

### **Fuel Card Categories**

33. There are two Defence fuel card types:
- a. Vehicle specific fuel card. A fuel card that is specifically assigned to and used against a specific vehicle or aircraft
  - b. Generic fuel card. A fuel card that is not assigned to a specific vehicle or aircraft. Can be used for equipment such as plant, generators and loan pool vehicles.
34. There are two Defence fuel card categories:
- c. Commercial (e.g. Shell, BP, Caltex) that can be used at specific commercial service stations and Defence Petrol, Oils and Lubricants (POL) sites; and
  - d. Defence on-base (white cards with a Defence logo) cards that can only be used at Defence POL sites fitted with FUELSCAN.
35. In general, commercial fuel cards are vehicle or aircraft specific with embossed vehicle or aircraft registration on the fuel card. There is an agreed need for generic commercial cards to accommodate the provision of fuel for minor items of Plant and allocated Loan Pool vehicles. Generic fuel cards are considered to carry higher level of fraud risk as they are able to be used on any vehicle/equipment and purchase any type of fuel.
36. The table below provides a profile of relevant fuel use cases and how they are aligned with customer activity, Defence vehicle type and fuel card type. This profile should be used together with Fuel Card Entitlement rules at paragraph 28 to determine the appropriate number and type of fuel cards permitted.

<b>Fuel Use Cases</b>	<b>Customer Activity</b>	<b>Defence Vehicle Type (white/green)</b>	<b>Fuel Card Types</b>
<b>Ground Fuel Cards</b>			
Unit travel	Travel interstate for site visits or seminars conferences,	White vehicles	Vehicle specific

	meetings etc		
Exercises	Military exercises	Plant & Equipment white/green vehicles	Generic vehicle specific
Operations	Military operations	White/green vehicles	Vehicle specific
Transport unit (People, medical runs)	Transport military/civilians from sites	White vehicles	Vehicle specific
Repair unit	Pick up vehicle parts	White vehicles	Vehicle specific
Loan pool vehicles	Varied	White/green vehicles	Vehicle specific and/or generic
Emergency use ( in circumstances where vehicle specific fuel card has been cancelled or damaged)	Varied	White/green vehicles	Generic
Equipment use (Ground Support Equipment (GSE))	Varied	Plant & Equipment	Generic
<b>Aviation Fuel Cards</b>			
Training unit	Training pilots, training for war	Aircraft	Vehicle (tail Number) specific
Operations (border security, search and rescue operations)	Deployment	Aircraft	Vehicle (tail number) specific

37. White vehicles, green vehicles and Loan Pool vehicles are Defence plated vehicles. White vehicles include buses, tractors, coaches, sedans 4WDs and station wagons. All loan pool vehicles are owned and managed by Defence. Loan pool vehicles can be loaned out to units for a length of a day to a fortnight depending on the customer need.

## Fuel Card Entitlement

38. The table below identifies the basic entitlement for the issue of Defence fuel cards. These maximum entitlements may only be varied on the authority of the unit CO. The unit CO is responsible for ensuring that business cases associated with entitlement variation are forwarded to JFLA for consideration and retained within the unit for audit purposes. Requests for new cards are to be validated in accordance with this policy.

Commercial Fuel Cards			On Base Fuel Cards	
	Vehicle Specific	Generic	Vehicle Specific	Generic
Defence Vehicle	2 Cards	Nil	Nil	N/A
Individual Unit	Nil	Equal to 10% of vehicle holdings/borrowings	Nil	1 Card
Defence Aircraft	4 Cards	Nil	N/A	N/A

Hire/Lease Car

Nil

Nil

Nil

Nil

## **Transaction Limits**

39. Vehicle specific cards have a financial transaction limit applied. The agreed limits imposed on all fuel cards are:
- BP - \$200.00 (soft limit per transaction)
  - Shell - \$300.00 (soft limit per transaction)
  - Caltex - \$300.00 (soft limit per transaction) - \$1000.00 (hard limit per transaction)

**Note:**

*If soft limit is breached, the transaction will still proceed. If the hard limit is breached the transaction will be declined.*

40. The supplier will send an email to the JFLA Fuel Cards inbox to flag any vehicle specific fuel card transactions that exceed the imposed limit. JFLA staff will then analyse the transaction and send a notification to the unit delegate requesting immediate justification/acceptance of the flagged transaction. All emails and responses are filed. A combined report is then compiled as part of the JFLA monthly Certificate of Compliance (COC).
41. Generic vehicle fuel cards will have a per transaction limit applied. This limit is to be determined and approved by the unit CO as part of the card application process. Unit CO are to be guided by expected card usage and fraud minimisation principles when determining this transaction limit.

## **Issuing Fuel Cards**

42. The following business rules apply to the issuing of Defence fuel cards:
- All Defence fuel cards must be requested, acquired and administered through ADOFMS;
  - ADOFMS Delegates must verify (on ADOFMS) all fuel cards within two months of issue;
  - Only ADOFMS delegates can request a new or replacement Defence fuel card
  - Defence fuel cards cannot be issued to contractors unless the supply of fuel by Defence is specified within a valid contract and the unit CO authorises the issue of a fuel card in direct support of that contract;
  - A unit CO must be an ADF member or a member of the APS;

- f. Defence fuel cards are not permitted to be provided to vehicles which are hired, leased or part of Defences Executive Vehicle Scheme;
  - g. Individual vehicles are to be allocated no more than two Commercial Defence fuel cards unless a business case is approved in accordance with paragraph 28.
43. It is mandatory for COs, ADOFMS delegates and all fuel card users to acknowledge their understanding and acceptance of roles and responsibilities in relation to their fuel card use and management, through signing of the following documents:
- a. CO to sign;
    - 1. ADOFMS Delegate registration, Removal or Change Form (AE153) - a copy to be submitted to JFLA and a copy to be retained by the delegate;
  - b. CO and ADOFMS Delegate to sign
    - 1. Acknowledgement by Unit Commanding Officer and ADOFMS Delegate of Conditions for Issue of a JFLA Fuel Card (AC101-2)
    - 2. All fuel card users must sign the Vehicle Authorisation and Task Form (AD049) or Generic Fuel Card Authorisation and Tasking Form (AE152)
44. All fuel card users must understand and accept the fuel card terms and conditions of use.
45. Primary responsibility for proper Defence fuel card use lies directly with the official who is issued with the card (i.e. card holder). ADOFMS delegates must ensure all Defence fuel card users are made aware of their responsibilities, and sign and return the appropriate forms as listed above.

### **Card Expiration**

46. All Defence fuel cards have an expiry date and cannot be used after this expiry date. Expired fuel cards will be automatically deactivated by the fuel supplier for commercial fuel cards or the Defence Fuel Card Systems Administrator for on base fuel cards. Expired fuel cards will not be automatically reissued by either the fuel supplier or the Defence Fuel Card Systems

Administrator. Should a replacement card be required, then ADOFMS Delegates will be required to request a replacement card in accordance with this policy.

47. The ADOFMS delegate is responsible for destroying (cutting/shredding) all expired fuel cards.

### **Fuel Card Data Maintenance**

48. With the exception of those transactions related to Aviation Fuel Cards all fuel card holdings and transactions must be recorded and managed in ADOFMS. The ADOFMS Website provides functionality to ADOFMSDelegates, to enable transaction reconciliation and data management. The ADOFMS Online Website Instruction Manual provides guidance to users of the ADOFMS Website and is available at [www.adofms.com.au](http://www.adofms.com.au) or through the above link.
49. ADOFMS Delegates are responsible for maintaining fuel card data in ADOFMS to ensure all fuel card, vehicle/aircraft and unit records in ADOFMS are accurate and that data is complete (i.e. unit/vehicle/aircraft registration, vehicle tank capacities etc) and reflect actual fuel card holdings of the unit.

### **Business Rules For Fuel Card Use**

50. The following business rules apply to the use of Defence fuel cards:
  - a. The use of the Fuel Card is subject to the requirements of;
    1. The Commonwealth Procurement Guidelines
    2. [Defence Procurement Policy Manual \(DPPM\)](#)
    3. [Defence Chief Executive Instructions \(CEI\) 2.3 - Defence Credit Cards](#)
    4. [DMO Chief Executive Instructions \(CEI\) 2.1 - Procurement and 2.3 Corporate Cards.](#)
  - b. The policy for the use and administration of Defence Fuel Cards managed by JFLA
  - c. Fuel card users are to undertake Simple Procurement training in accordance with the DPPM (refer to Simple Procurement -



Delegations, Competencies and Proficiencies) prior to the issue of any Fuel Cards

- d. Fuel cards are only to be used within the level of the financial limits approved for that Fuel Card.
- e. Fuel cards are not to be used for other than official Defence purposes.
- f. Fuel cards must only be used to purchase products allocated to that Fuel Card (If premium fuel is required to be activated against a fuel card, due to specification requirements of a vehicle, JFLA is to be approached for approval). No oil, retail or car wash transactions are to be made against Defence fuel cards.
- g. Vehicle specific fuel cards are required to have a valid registration number assigned to them.
- h. Vehicle specific cards cannot be used for vehicles other than for which the fuel card has been allocated to.
- i. All generic cards are to conform to a standard naming convention which includes the unit name and a sequential identifying number (e.g. JLU-N-001)
- j. Fuel cards that are not used for 12 months (with the exception of Approved Units, such as units involved with immediate response activities) or not verified by ADOFMS Delegate within two months will be cancelled by JFLA.
- k. If misuse of the Fuel Card occurs, i.e. used for purposes other than in accordance with the instructions given to a user, proceedings may be instituted against the user under Section 60 (1) of the FMA Act 1997 and if found guilty, the user may be liable for the maximum penalty of seven years imprisonment.
- l. Either the [AD049 Vehicle Authorisation and Task Form](#), or the [AE152 Generic Fuel Card Authorisation and Task Form](#) must be signed.

### **Retention And Record Keeping**

51. JFLA and Units (CO and ADOFMS delegates) are responsible for ensuring the compliance of record keeping and retention requirements of all paper and electronic documents set out in paragraphs 42-43. Documents must be kept for seven years after the record was prepared or obtained, in particular, evidence

supporting the fraudulent use of Defence fuel cards must be kept to facilitate fraud investigations.

52. The following business rules apply to the retention and record keeping procedures of Defence fuel cards:
  - a. Transactions for vehicle specific cards must be recorded on and validated against the specific Vehicle Authorisation and Task Form (AD049)
  - b. Transactions for a generic card (Commercial or on Base) must be recorded on and validated against the Generic Fuel Card Authorisation and Tasking Form (AE152)
53. Unit COs and ADOFMS delegates must retain the following paper and electronic documents to meet administrative needs for audit purposes.

Process	Documents to be retained for seven years
Appoint new ADOFMS delegate or change delegate	Acknowledgment by Unit CO and ADOFMS Delegate of conditions for issue of a JFLA issued Fuel Card (AC101-2)
Fuel card entitlement	ADOFMS Delegate Registration, Removal or Change Form (AE153)
Monthly fuel card usage and reconciliation	Business Case Vehicle Authorisation and Task Form (AD049)
	Generic Fuel Card Authorisation and Task Form (AE152)
Transaction dispute and resolution process	Supplier Receipts Vehicle Authorisation and Task Form (AD049)
	Generic Fuel Card Authorisation and Task Form (AE152)
	Supplier Receipts
Cancellation of Fuel cards	Documents supporting the follow up and resolve of disputable items Confirmation of cancellation email from ADOFMS
Monthly exception reporting	Evidence of review and actions taken in relation to all exception reports provided by JFLA
Annual validation and review of fuel card holdings	Completed annual validation of fuel card holdings form prepared by ADOFMS delegates

signed by Unit CO

## **Fuel Card Misuse and Fraud**

54. All fuel card users, ADOFMS delegates, COs and JFLA staff are responsible for ensuring the proper control and use of Defence fuel cards and must sign the relevant document or form that acknowledges their acceptance of their fuel card use and management role and responsibilities as detailed in paragraph 33.
55. Responsibilities of fuel suppliers in relation to Defence fuel card misuse and fraud will be managed through contract terms and conditions.
56. Fraudulent use of Defence fuel cards perpetrated by staff (internal fraud) or by persons outside the organisation (external fraud) is an offence under various provisions of the Crimes Act 1914 and Criminal Code Act 1995.
57. Commercial Defence fuel cards are deemed to be a credit card and are bound by the regulations applicable to Commonwealth provided credit cards. Internal fraud also constitutes misconduct under the APS Code of Conduct and Defence Force Discipline Act (1982) and the Financial Management and Accountability Act 1997 - Section 60 (Misuse of Commonwealth Credit Cards) provides for imprisonment of up to seven years for misuse (fraudulent) use of Commonwealth credit (or fuel) cards.
58. Reasonable suspicions or allegations of fraudulent use of Defence fuel cards constitutes a Notifiable Incident (NI) and must be reported immediately through line management to JFLA and the responsible Division Head and managed in line with the requirements set out in DI (G) ADMIN 45-2 - The Reporting and Management of Notifiable Incidents, which sets out the mandatory reporting procedures. Matters will be referred to the Assistant Secretary General Investigation and Review, and matters involving Service personnel should also be referred to the Australian Defence Force Investigative Services (ADFIS). The mandatory reporting of an NI is an obligation that applies to all Defence personnel at all times, and failure to comply with the mandatory aspects of this instruction may result in administrative or disciplinary action.

59. DI (G) PERS 45-5 Defence Whistleblower Scheme sets out an individuals rights and responsibilities under the Defence Whistleblower Scheme. Matters of misconduct or unethical behaviour, fraud, or other activity that breaches Commonwealth legislation, waste and abuse of Defence resources can be reported to the confidential 24 hour whistleblower hotline - 1800673502. Contractors working for Defence may also use the scheme. Information on, or queries relating to investigations or the scheme are available from the Director Investigations and Recovery on (02) 6266 4322.

### **Audit and Review Guidelines**

60. The following guidelines have been developed to assist unit level personnel execute their audit and review requirements. Documents that must be maintained to provide evidence of the performance of these activities are detailed in paragraph 43.
61. All Defence fuel card transactions will be captured and managed in ADOFMS. This will assist JFLA in the performance of fraud data analysis. Fuel cards must not be recorded and managed manually on excel spreadsheets, or anywhere other than in ADOFMS.

### **Validating and Reconciling Transactions**

62. ADOFMS Delegates are to confirm that transactions have occurred and are to validate the appropriateness of each transaction, as determined in this policy. ADOFMS delegates must reconcile all fuel card transactions generated by cards allocated to them, within 30 days of the end of month in which the transaction occurred. Any fuel cards which show outstanding transactions that have not been reconciled within 90 days of the of the month in which the transaction occurred, will be immediately canceled and the Unit CO advised accordingly.
63. ADOFMS delegates are responsible for investigating and validating any irregular or abnormal activity, which is identified in those reports listed at paragraphs 17 and 55.
64. ADOFMS delegates shall perform the following tasks to verify the validity of each transaction:

- a. Check that transaction listings in ADOFMS match supplier receipts (i.e. fuel supplier, date of transaction, litres used, value of the transaction)
- b. For vehicle specific fuel cards, match transactions to the Vehicle Authorisation and Task Form (AD049)
- c. For generic fuel cards, match transactions to the Generic Fuel Card Authorisation and Tasking Form (AE152)
- d. Accept transactions in ADOFMS where supplier receipts match corresponding authorisation task forms
- e. Dispute transactions in ADOFMS where supplier receipts or ADOFMS records do not match corresponding authorisation and task forms
- f. Resolve disputed transactions with fuel suppliers in a timely manner.

### **Abnormal and Unreconciled Transactions**

65. ADOFMS delegates shall address and resolve abnormal transactions detailed in the following exception reports which JFLA will supply on a monthly basis

Exception Report from JFLA	ADOFMS Delegate Actions Required
1 Vehicle specific fuel cards incurring multiple transactions on the same day	Investigate the cause of these multiple transactions and take disciplinary action if required
2 Transactions greater than vehicle capacity	Investigate the cause of these transactions and take disciplinary action if required
3 Unreconciled transactions (defined as transactions which are more than 30 days old)	ADOFMS delegates must reconcile all fuel card transactions generated by cards allocated to them, within 30 days of the end of the month in which the transaction occurred
4 Unverified fuel cards with transactions	ADOFMS delegate to investigate immediately and mark as reconciled or in dispute

### **Fuel Card Holdings**

66. On a monthly basis, JFLA will provide the exception report shown below to ADOFMS delegates, so that delegates can assess the ongoing need for fuel cards. Fuel cards must be

cancelled where a valid requirement to renew the card does not exist or has not been approved.

Exception Report from JFLA	ADOFMS Delegate Actions Required
Fuel card expiring within 2 months	Re-assess the need for reordering expired fuel cards

67. Each year the ADOFMS delegate must reconcile Unit fuel card holdings against Unit records maintained in ADOFMS. This is to ensure that all fuel cards have a corresponding fuel card record in ADOFMS and that all fuel cards listed in ADOFMS exist and are accounted for. This reconciliation shall be reviewed and signed off by the CO using the Annual Validation of Fuel Card Holdings Form; available from the JFLA website. The reconciliation form is to be retained by the unit and any discrepancies reported to JFLA for investigation.

### Commanding Officer Responsibilities

68. COs are ultimately accountable for the appropriate validation of all fuel card transactions and must regularly ensure ADOFMS delegates are performing reconciliations appropriately, reviewing exception reports and resolving abnormal or unreconciled transactions in accordance with this policy. In making this assessment, the unit CO should also ensure ADOFMS delegates have adequate skills, receives the appropriate level of training, and have sufficient time available to perform their fuel card management duties.
69. JFLA will provide the following exception reports to unit COs to facilitate their review and oversight responsibilities:

	Exception Report From JFLA	CO Actions Required
1	Delegate with transactions exceeding 500 per month	Assess whether the delegate can continue to perform their duties effectively in view of their transaction workload
2	Aging dispute transaction (defined as transactions which remain unresolved for more than 30 days from the date they were first disputed)	Investigate aging dispute and take immediate action to resolve with the Fuel supplier and Defence Fuel Card Systems Administrator

70. Unit COs are responsible for the effective implementation of Defence fuel card controls as developed by JFLA and as set out in this policy and the Defence Fuel Card Fraud Control Plan (FFCP) V05S07C01B2

71. Unit COs must sign off the Annual Validation of Fuel Card Holdings Form prepared by ADOFMS Delegates each year, which reconciles actual fuel card holdings to records maintained in ADOFMS to ensure all fuel cards listed in ADOFMS exist and are accounted for.
72. Unit COs must validate any transactions relating to the ADOFMS delegates direct use of fuel cards against supplier receipts and vehicle/generic fuel card authorisation and task forms. ADOFMS Delegates must reconcile these transactions in ADOFMS, but only the unit Co can validate the transaction. This is important for maintaining appropriate segregation of duties.

## **IMPLEMENTATION**

73. All organisations and personnel involved in any aspect of Defence fuel cards usage and management must have access to this policy document, be familiar with the contents of this policy document, and must strictly adhere to the policy requirements to ensure proper control and use of Defence fuel cards. This includes Defence fuel card users, ADOFMS delegates, COs, JFLA personnel and Defence personnel and contractors.
74. Mandatory forms required for the management of Defence fuel cards are as follows:
  - a. Form AE153 ADOFMS Delegate Registration, Removal or Change
  - b. Form AC101-2 Acknowledgement by Unit Commanding Officer and ADOFMS Delegate of Conditions for issue of a JFLA issued Fuel Card
  - c. Form AD049 Vehicle Authorisation and Task Form
  - d. Form AE152 Generic Fuel Card Authorisation and Tasking
  - e. Annual Validation and Review of Fuel Card Holdings - Available on the JFLA website  
<http://intranet.defence.gov.au/dmoweb/sites/JFLA/>

## **DELEGATIONS**

75. For routine administration of Defence fuel cards, fuel card data and ADOFMS issues, contact:

Transponder Technologies  
Telephone: (08) 8215 5030  
Email: [support@adofms.com.au](mailto:support@adofms.com.au)

76. For any other fuel card management issue contact:

JFLA Fuel Card Manager  
Telephone: (02) 9393 3311  
Email: [jfla.fuelcards@defence.gov.au](mailto:jfla.fuelcards@defence.gov.au)

## COMPLIANCE

77. All organisations and personnel involved in any aspects of the Defence fuel cards use and management process must comply with the policy for the use and administration of Defence Fuel Cards managed by the Joint Fuel and Lubricants Agency; this includes Defence personnel and contractors that operate as Defence fuel card users, ADOFMS delegates, COs and JFLA staff.

## RELATED DOCUMENTS

78. The following documents, policies and legislation inform the Defence Fuel Card Policy:

- a. The Commonwealth Procurement Guidelines
- b. [Defence Chief Executive Instructions \(CEI\) 2.3 Defence Credit Cards](#)
- c. [DMO Chief Executive Instructions \(CEI\) 2.1 Procurement and 2.3 Corporate Cards](#)
- d. [Defence Fuel Card Fraud Control Plan V05S07C01B2](#)
- e. [Defence Procurement Policy Manual](#)
- f. Defence Instructions (General) ADMIN 45-2 The Reporting and Management of Notifiable Incidents
- g. Financial Management Act 1997 section 60
- h. APS Code of Conduct
- i. Defence Force Discipline Act (1982)



## Defence Road Transport Instructions

**Process: 8.0 Inventory Management  
(JFLA/UNIT)**

<b>UNIT:</b>	0
<b>Visit Date:</b>	0

Update Statistics on Team Leader  
& Executive Summary Sheet

### Objective

To gain assurance that the Units Inventory Management process is being performed in accordance with the ESCM.

### Testing procedures

Auditor's should use a number of tools to form their assessment including but not limited to: physical evidence/reports/observations and discussions with staff and contractors. Testing is to be performed by Defence's Compliance & Assurance teams. The obje

**Auditors  
Name:**

**Discussion held with:**

### 8.1 Management Process

**Method: Conduct an open interview with the manager/supervisor responsible asking them to describe the process to gain confirmation each step in the process is being performed correctly.**

BPT ID	ID	Audit Observations (the auditor is to confirm the following processes are occurring on site)	Result	Additional Comments
8.1.01	KPS	Daily and weekly fuel dips are to be conducted are to be recorded in JFIMS.	N/A	

8.1.02	KPS	All tanks to be dipped 3 times in a 5 minute interval, end of week for fuel dip transactions is COB Wednesday and dips to be conducted first thing on Thursday.	N/A	
8.1.03	KPS	All discrepancies are to be investigated, and those above tolerance levels are to be referred to JFLA.	N/A	
8.1.04	KPS	Above ground storage tanks which are not in regular use, as a minimum must be dipped monthly.	N/A	

Discussion held with:

### 8.3 Management Controls

**For BPT testing of WEEKLY/MONTHLY/QUARTERLY REPORTS:** For all reports identified for Desk Top Review (DTR), the testing team is to identify aged transactions to determine if the business unit is compliant and is scored accordingly. The score is based on age profiling only, if the business unit has written evidence to resolve the line and/or report, the team leader is to note the action by the business unit in the FINDINGS column as an observation only, however, the score will remain unchanged. **NOTE:** When reviewing the action by the business unit on reports identified for DTR review, the testing team is to record in the FINDINGS column if the action by the business unit has been repeated by reviewing a number of reports.

Sample Details												
BPT ID	ID	Control Activity	Role Responsible	Document Reference	USER HOW TO DEMONSTRATE CONTROL	USER GUIDANCE	Testing and Sampling Method	Score	Finding s (include Evidence Reference Number, the format is eg 8.2.1.A, 8.2.1.B etc)	Actions Required to Achieve Compliance & Any Additional Comments	Action Owner	Expected re-test date

8.2.01	<b>KEY BUSINESS CONTROL</b>  <b>UNIT ONLY</b>	Ensure daily/weekly/monthly dips are entered into Fuels Manager.	Unit JFIMS Manager/Manager ADF POL Site	ESCM 12.02.01 ESCM 04.08.21	The Manager ADF POL Site is to ensure that monthly dips are entered into Fuels Manager ledger.  Fuel Dip records are to be retained for five years.	Fuel Dipping is to be conducted: 1. UST and AST - General, weekly and monthly. 2. UST - Specific, daily and weekly. 3. AST - Specific, weekly. 4. AST - not in regular use, monthly.	From the selected sample, the testing team is to verify the Fuel Dip recordings are recorded correctly in JFIMS (pending Tank Type). Fuel Dip recordings are to be for individual tanks, if Fuel Dip recordings are consolidated for the Fuel Facility, the Control is scored NON-COMPLIANT.  <b>NOTE: Fuel Dip readings can be taken from a Reconciliation LOG or other authorised alternative.</b>	N/A				
--------	---	--	---	--------------------------------	---	--	--	-----	--	--	--	--

Discussion held with:

### 8.3 Management Controls

**For BPT testing of WEEKLY/MONTHLY/QUARTERLY REPORTS:** For all reports identified for Desk Top Review (DTR), the testing team is to identify aged transactions to determine if the business unit is compliant and is scored accordingly. The score is based on age profiling only, if the business unit has written evidence to resolve the line and/or report, the team leader is to note the action by the business unit in the FINDINGS column as an observation only, however, the score will remain unchanged.

**NOTE:** When reviewing the action by the business unit on reports identified for DTR review, the testing team is to record in the FINDINGS column if the action by the business unit has been repeated by reviewing a number of reports.

BPT ID	ID	Control Activity	Role Responsible	Document Reference	USER HOW TO DEMONSTRATE CONTROL	USER GUIDANCE	Testing and Sampling Method	Sample	Score	Finding s (include Evidence Reference Number, the format is eg 8.3.1.A, 8.3.1.B etc)	Actions Required to Achieve Compliance & Any Additional Comments	Action Owner	Date Expected To Be Compliant
8.3.01	KEY BUSINESS CONTROL JFLA ONLY	The Waste Fuel Disposal Report is actioned on a monthly basis.	JFLA LSA	SOP (JFLA-04-0-004)	The Waste Fuel Disposal Report is actioned on a monthly basis. The JFLA LSA is to review and investigate any anomalies.  The report is to be retained in a central location for a period of seven years.		The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the		N/A	(HINT: How many lines outstanding/oldest line)			

							<p>score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p> <p>For Retail Units - Between 30 - 60 days the score = 4 (GREEN) Compliant - Between 61 - 90 days the score = 2 (AMBER) Unit to remediate - Greater than 90 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p>						
--	--	--	--	--	--	--	---	--	--	--	--	--	--

8.3.02	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Active fuel cards not used for 12 months Report (with the exception of Approved Units, such as units involved with immediate response activities) is actioned monthly.	JFLA/JSC	ESCM 05.07.01B	<p>In accordance with the JFLA fuel card audit schedule, a sample of transactions from each Exception Report is selected for validation.</p> <p>The report and sample transactions which have been validated are to be retained in a central location for a period of seven years.</p>	Forward report to JSC for cancellation of fuel card in ADOFMS and notify ADOFMS delegate that the fuel card has been cancelled and should be physically destroyed	<p>The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p> <p>For Retail Units - Between</p>		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	--	----------	-------------------	--	---	--	--	-----	--	--	--	--



8.3.03	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Active fuel cards not verified for two months Report is actioned monthly.	JFLA/JSC	ESCM 05.07.01B	<p>In accordance with the JFLA fuel card audit schedule, a sample of transactions from each Exception Report is selected for validation.</p> <p>The report and sample transactions which have been validated are to be retained in a central location for a period of seven years.</p>	Forward report to JSC for cancellation of fuel card in ADOFMS and notify ADOFMS delegate that the fuel card has been cancelled and should be physically destroyed.	<p>The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p> <p>For Retail Units - Between</p>		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	--	----------	-------------------	--	--	--	--	-----	--	--	--	--



							30 - 60 days the score = 4 (GREEN) Compliant - Between 61 - 90 days the score = 2 (AMBER) Unit to remediate - Greater than 90 days the score = 0 (RED) Tier 3/LAB to escalate to 1*							
--	--	--	--	--	--	--	---	--	--	--	--	--	--	--

8.3.04	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Active fuel cards without a unit Report is actioned monthly.	JFLA/JSC	ESCM 05.07.01B	<p>In accordance with the JFLA fuel card audit schedule, a sample of transactions from each Exception Report is selected for validation.</p> <p>The report and sample transactions which have been validated are to be retained in a central location for a period of seven years.</p>	Forward report to JSC for cancellation of fuel card in ADOFMS.	<p>The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p> <p>For Retail Units - Between</p>		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	--	----------	-------------------	--	--	--	--	-----	--	--	--	--



8.3.05	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Cancelled fuel cards with transactions Report is actioned monthly.	JFLA	ESCM 05.07.01B	<p>In accordance with the JFLA fuel card audit schedule, a sample of transactions from each Exception Report is selected for validation.</p> <p>The report and sample transactions which have been validated are to be retained in a central location for a period of seven years.</p>	Forward report to ADOFMS delegate to resolve with fuel supplier and Defence Fuel Card Systems Administrator.	<p>The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p> <p>For Retail Units - Between</p>		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	---	------	-------------------	--	--	--	--	-----	--	--	--	--



8.3.06	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Unreconciled transactions Report is actioned monthly.	JFLA	ESCM 05.07.01B		Send report to ADOFMS delegate to reconcile transactions within the specified time period.	The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*  For Retail Units - Between		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	---	------	-------------------	--	--	--	--	-----	--	--	--	--

--	--	--	--	--

	30 - 60 days the score = 4 (GREEN) Compliant - Between 61 - 90 days the score = 2 (AMBER) Unit to remediate - Greater than 90 days the score = 0 (RED) Tier 3/LAB to escalate to 1*						
--	---	--	--	--	--	--	--

8.3.07	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Unverified fuel cards with transactions Report is actioned monthly.	JFLA	ESCM 05.07.01B	<p>In accordance with the JFLA fuel card audit schedule, a sample of transactions from each Exception Report is selected for validation.</p> <p>The report and sample transactions which have been validated are to be retained in a central location for a period of seven years.</p>	Send report to ADOFMS delegate to verify card in ADOFMS and confirm validity of transaction.	<p>The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p> <p>For Retail Units - Between</p>		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	--	------	-------------------	--	--	--	--	-----	--	--	--	--





8.3.08	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Delegate pairs with more than 500 transactions per average month (per quarter) Report is actioned monthly.	JFLA	ESCM 05.07.01B	In accordance with the JFLA fuel card audit schedule, a sample of transactions from each Exception Report is selected for validation.  The report and sample transactions which have been validated are to be retained in a central location for a period of seven years.	Send report to CO to determine whether ADOFMS delegate has sufficient capacity to appropriately review all transactions within the month, or alternatively create a second unit.	The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*  For Retail Units - Between		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	---	------	-------------------	---	--	--	--	-----	--	--	--	--

							30 - 60 days the score = 4 (GREEN) Compliant - Between 61 - 90 days the score = 2 (AMBER) Unit to remediate - Greater than 90 days the score = 0 (RED) Tier 3/LAB to escalate to 1*							
--	--	--	--	--	--	--	---	--	--	--	--	--	--	--

8.3.09	<b>KEY BUSINESS CONTROL</b>  <b>JFLA ONLY</b>	Aging Dispute Transaction (remain unresolved for more than 30 days from the date they were disputed) Report is actioned monthly.	JFLA	ESCM 05.07.01B	<p>In accordance with the JFLA fuel card audit schedule, a sample of transactions from each Exception Report is selected for validation.</p> <p>The report and sample transactions which have been validated are to be retained in a central location for a period of seven years.</p>	Forward report to CO to investigate aged dispute transaction with fuel supplier.	<p>The testing team is to undertake a DTR to validate the oldest line within the following parameters: For Wholesale Units - Between 30 - 90 days the score = 4 (GREEN) Compliant - Between 91 - 180 days the score = 2 (AMBER) Unit to remediate - Greater than 180 days the score = 0 (RED) Tier 3/LAB to escalate to 1*</p> <p>For Retail Units - Between</p>		N/A	(HINT: How many lines outstanding/oldest line)			
--------	---	--	------	-------------------	--	--	--	--	-----	--	--	--	--





## **Annex D Fuel Control Framework Current**

### **BUSINESS PROCESS TESTING FRAMEWORK**

#### **INTRODUCTION**

1. The internal audit function provides an independent and objective review to management that the designed financial and logistics controls are managing the organisation's risks and achieving their objectives. This also ensures that the Key Business Process Controls are operating in an efficient and effective manner as well as assisting management in improving organisational performance.
2. The evidence-based approach is used in audits to reach reliable and re-performable audit conclusions in a systematic audit process. Evidence will be collected on Key Business Process Controls for both preventive and detective controls.

#### **AIM**

3. The aim of this chapter is to describe the framework adopted by Defence Logistics Compliance and Assurance Network Teams to conduct Business Process Testing (BPT) and to outline the relevant testing standards, templates and reporting requirements that apply.

#### **AUTHORITY**

4. The ESCM is authorised jointly by the Secretary and the Chief of the Defence Force (CDF) IAW [DI\(G\) LOG 4-1-002](#).

#### **SCOPE**

5. The scope of this chapter is to state the BPT framework for the Defence Logistics Compliance and Assurance Network.

### **BUSINESS PROCESS TESTING FRAMEWORK**

6. The BPT is a means by which compliance and assurance with Defence supply chain policies and procedures is ascertained, and in conjunction with other control frameworks, is a part of the Defence Inventory Assurance Strategy (IAS). The BPT framework consists of the following elements that are described in more detail in subsequent paragraphs:

- a. High Impact Unit List.
- b. BPT Requirement and Frequency Determination.
- c. BPT Tool.
- d. BPT Reliance Key.

## **HIGH IMPACT UNIT LIST (FORMERLY HIGH MATERIALITY LIST)**

- 7. As part of the Defence Inventory Assurance Strategy, each year Logistics Assurance Branch (LAB) identifies Business Units that are likely to have a high impact on the accuracy of the Defence Asset and Inventory Accounts held in MILIS. This list is published annually as the High Impact Unit List (HIUL).
- 8. Factors taken into account when developing the HIUL are:
  - a. Value of Inventory and Assets held (or managed) by Business Units and System Project Offices (SPOs). This includes warehouse and SCA holdings.
  - b. BPM Results.
  - c. NAIS outcomes.
  - d. Most recent BPT result.
  - e. Stocktake results.
  - f. Input from key stakeholders.
- 9. Materiality for other Logistics Information Systems (LIS) will be selected from the respective Logistics Information Systems (eg SLIMS).

## **BPT REQUIREMENT AND FREQUENCY DETERMINATION**

- 10. BPTs are scheduled by financial year in conjunction with the Group or Service Tier 3. BPTs can also be included into the schedule/ when required by LAB and on request by AFCD or ANAO.
- 11. The frequency for the conducting a MILIS BPT at a BU is:
  - a. Business Units on the High Impact Unit List (HIUL);
    - 1. Within the current financial year.
  - b. Business Units that operate one or more MILIS warehouses:



1. Once every three years if the Business Unit has no more than four BPM red traffic lights on the same controls consecutively over three months; or
  2. If the Business Unit has five or more red BPM KPI traffic lights on the same controls consecutively over three months. A BPT is to be scheduled by T3 within 18 months of occurrence.
12. The requirement for a SLIMS BPT to be conducted is determined by the following:
- a. Major Fleet Units (MFUs) and Minor Warfare Vessels (MWVs) using SLIMS:
    1. MFUs and MWVs identified on the HIUL will be subject to a Departmental Management Audit (DMA) / BPT annually.
    2. MFUs or MWVs that are not on the HIUL with ongoing poor results will be considered by Director General Logistics – Navy (DGLOG–N), in consultation with the Executive Director Logistics Assurance (EDLA) as a high compliance and assurance risk, at which time they will be considered for inclusion on the HIUL and will be assessed annually.
    3. Where a MFU or MWV has received a BPT score of 50 percent or less and/or has eight or more CARs raised, the ship is to be notified that another abridged DMA focusing on logistics will be conducted within 9 months of the initial DMA. This DMA will be subject to availability and operational tasking of the MFU or MWV.

#### Note

*Where a MFU or MWV has not achieved a suitable standard, the additional logistics focused DMA will be an added audit impost. It is not required if the DMA and BPT for a ship is above the 50 percent BPT Key Performance Indicator (KPI) and below the eight CAR KPI. It is designed to serve as an incentive for the MFUs and MWVs to ensure compliance with logistics procedures.*

- b. The minimum frequency for SLIMS BPT/DMA is 2 years (excluding any time in refit or deep maintenance).

13. Where Business Units have multiple warehouses under their management, Groups and Services' Tier 3 are to determine if the BU is to be tested as a complete entity or the testing limited to specific warehouses that are considered to pose the highest risks. Groups and Services are to advise LAB of details when the option of limiting the BPT to specific warehouses has been selected.
14. BPTs for units on the High Impact Unit List or those triggered by BPM KPI breaches are to be tested against all processes applicable to the Business Unit.
15. The above frequency is the minimum requirement to meet an appropriate level of governance. Groups and Services are to conduct a risk assessment on their Business Units and can schedule more frequent BPTs if their risk assessment or internal procedures warrant. Factors that can be taken into account in the risk assessment include (but are not limited to):
  - a. Previous BPT Results.
  - b. BPM KPI results or trends.
  - c. Stocktake results.
  - d. NAIS or other audit results.
  - e. Staff turn-over or unit relocation
16. Groups and Services are to develop an annual Financial year BPT Schedule and advise details to LAB by 01 August each year. LAB staff will consolidate the individual schedules into an overall Defence schedule and advise details of LAB staff participation/observation in specific BPTs. Amendments to the Group and Service schedules are to be advised to LAB within one month of being identified.

## 17. BUSINESS PROCESS TESTING TOOL

18. C&A testing is conducted, and results recorded, using a structured BPT Tool. There are currently two formats of the BPT Tool available:

- a. On-line BPT Tool – accessed from the [LAB DLPM BPT Webpage](#) or from the link in ESCM [V10S03C06](#). This format is currently used for MILIS and SLIMS.
- b. Manual (Excel spreadsheet) BPT Tool – accessed from the relevant ESCM chapter in V10S03 and is currently used by Fuel Services and Explosive Ordnance Branches for JEFMS and COMSARM BPTs.

19. Both of these BPT tools comprise of three segments as follows:

- a. Business Management Practices (BMP). The BMP segment of the BPT contains a list of the most important steps in a business process, omission of which would affect completion of the process. The BMP is conducted as a walk through of the business process with the unit representative to provide the auditor with an understanding of how the process is conducted at the site, to provide an understanding of any local variations and to identify if there are any significant steps that are being missed. The tester will use a range of tools to assist them to make an assessment. These can include physical evidence, reports, observations, discussions with staff and any previous BPT results.
- b. Key Business Process Controls (BPC). These are controls within each of the business process segments that pose a significant financial or supply chain impact on the business process. Physical testing of transactions and reports is conducted to determine if the process is operating in accordance with the ESCM.
- c. Business Management Controls (BMC). Testing of Management Reporting. This activity tests a range of system reports to determine if relevant action has been taken by the Business Unit to correct any transaction exceptions identified by the reports. (This section is replaced by a Business Process Monitoring (BPM) Dashboard for MILIS.

20. The BPT Tool has been designed to manage both Preventative and Detective controls within each of the Business Processes conducted at Business Units.

### **Preventive Controls**

21. Preventative controls are applied during the normal flow of logistics transactions to identify any breakdown in the business process being tested. This is to prevent occurrence of error or fraud that could lead to misstatement of General Stores Inventory (GSI) or Military Support Item (MSI) balances.

### **Detective Controls**

22. Detective controls are used to assist in identifying any process errors, data errors or faults, including procedural faults or miss appropriation of assets that may have occurred.

### **BPT Reporting**

23. BPTs have a Quality Assurance (QA) review by the Tier 3. When the QA is completed, the BPT is to be submitted to LAB within 10 working days of the BPT being conducted. Completed BPTs are to be submitted as follows:
  - a. On-line BPT Tool. Completed BPTs are to have their status updated to 'with LAB' and an electronic copy of completed sample sheets and supporting evidence for any non-compliances placed in the LAB objective folder for the Group or Service.
  - b. Manual BPT Tool. Electronic copies of completed manual BPT spreadsheets, completed sample sheets and supporting evidence for non-compliances are to be placed in the LAB objective folder for the Group or Service. The relevant BPT coordinator is to be advised of completion. NOTE: Manual BPTs are only to be used for JFMS and COMSARM systems.

## BPT RELIANCE KEY

24. A BPT Reliance Key is used by Defence to support measurement and reporting of compliance levels across Groups and Services. The key is used to report compliance levels for a BU at the conclusion of each BPT (via the Executive Summary Report) and at a summary level by process and Group or Service on a periodic basis. The threshold for BPT compliance is 85%.

Percentage	Level of Reliance
0.00% - 49.99%	No Reliance
50.0% - 74.99%	Low Reliance
75.0% - 84.99%	Moderate Reliance
85.0% - 100%	High Reliance

1. TABLE 1: BPT RELIANCE KEY

Control Activity	Role Responsible	Testing and Sampling Method
Ensure the Defence Fuel Card is maintained for the vehicle/asset.	Unit Transport Manager/SG Fleet	From the selected sample, the testing team is to verify the Defence Fuel Card is maintained for the vehicle/asset: (1) the correct Defence Fuel Card is allocated to the vehicle/asset, (2) any outstanding Exceptions over 30 days has an investigation in pro
Ensure the AD049 Vehicle Log is maintained for the vehicle/asset.	Unit Transport Manager	From the selected sample, the testing team is to verify the AD049 Vehicle Log is maintained for the vehicle/asset for the past 12 months, when the vehicle/asset was in use: (1) all the driver's details clear, coherent and all details completed in the AD04
The Waste Fuel Disposal Report is actioned on a monthly basis.	FSB LSA	The testing team is to undertake a DTR to validate the the oldest line within the following parameters: For Wholesale Units <ul style="list-style-type: none"> <li>- Between 30 - 90 days the score = 4 (GREEN) Compliant</li> <li>- Between 91 - 180 days the score = 2 (AMBER) Unit to remediate</li> </ul>
Aging Dispute Transaction (remain unresolved for more than 30 days from the date they were disputed) Report is actioned monthly.	FSB	The testing team is to undertake a DTR to validate the the oldest line within the following parameters: For Wholesale Units <ul style="list-style-type: none"> <li>- Between 30 - 90 days the score = 4 (GREEN) Compliant</li> <li>- Between 91 - 180 days the score = 2 (AMBER) Unit to remediate</li> </ul>
The Invalid ODO Reading Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0</li> </ul>

Control Activity	Role Responsible	Testing and Sampling Method
		(RED) Teir 3 / FSLAB to escalate to 1*.
The Excessive Fuel (Overfill) Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
The Recent Infringements Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
The Fuel Cards Being Used More Than 3 Times in a 24 Hr Period Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
The Inactive Fuel Cards Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
Ensure the Annual Census was conducted and the results sent to SG Fleet.	Unit Transport Manager	The testing team is to validate when the last Annual Census was conducted. The testing team is to validate: <ol style="list-style-type: none"> <li>All Defence Fuel Cards were reconciled.</li> <li>Evidence of remediation for anomalies.</li> <li>Email confirmation to SG Fleet of completion of the Census</li> </ol>

Corporate Card

Quality Assurance Manual

### Quality Assurance Manual Approval:

Endorsed by:

Name: Scott Taylor  
Title: Manager CCSC  
Organisation: CFO  
Corporate Card Support Centre

Approved by:

Name: Glenn Johnston  
Title: Director  
Organisation: CFO  
Finance Business Centre

### Quality Assurance Manual Version Control

<b>Objective ID</b>	AF8300083
<b>Version Number</b>	0.4
<b>Issue Date</b>	
<b>Due for Review</b>	

### Change History

<b>Version</b>	<b>Issue Date</b>	<b>Author</b>	<b>Reason for Change</b>
1		Troy Larke	Creation of new Manual to include all SOPs and QA Material
2	22 Jan 2013	Troy Larke/Scott Taylor	Annual update
3	7 May 2013	Troy Larke	Update to QA 2.1.13
4	26 August 2013	Troy Larke	Update to QA 2.1.13



<b>1.</b>	<b>CORPORATE CARD QUALITY ASSURANCE MANUAL.....</b>	<b>1</b>
1.1	Back Ground and Purpose .....	1
1.2	Manual Scope.....	1
1.3	Review Frequency .....	1
1.4	Manual Overview .....	1
1.5	Responsibility .....	1
2.1	Corporate Card Quality Assurance Plan.....	2
2.1.1	User - QA New Users (Self Registered) .....	3
2.1.2	User - Enterprise Controller Report .....	5
2.1.3	User - Admin Centre Controller Report .....	5
2.1.4	User - Contractor Report.....	6
2.1.5	User - Employee Users Not on PMKeys .....	6
2.1.6	User - Locked Users with Active Cards.....	7
2.1.7	User - Locked Users with Unprocessed Transactions .....	7
2.1.8	Card - Active cards not on PMKeyS.....	8
2.1.9	Card – More than One Active Card (Same Company Code).....	8
2.1.10	Card – High Limit Cards ( $\geq$ \$250,000) .....	9
2.1.11	Card – Report Group/Company Check.....	9
2.1.12	Card – Missing EID or Email .....	10
2.1.13	Card – Defence and DMO Card Holders - DTC .....	10
2.1.14	Card – Defence and DMO Card Holders - DPC .....	10
2.1.15	Card - Cards not on ProMaster.....	11
2.1.16	Card – Cash Access Cards .....	11
2.2	Suspected Fraud or Misuse.....	13
<b>3.</b>	<b>CMS SYSTEM &amp; ACCOUNT ADMINISTRATION .....</b>	<b>15</b>
3.1	CMS Systems Operations.....	15
3.2	Process DTC Applications.....	17
3.3	Process DPC Application .....	19
3.4	Appoint Authorising Officer (NAB).....	21
3.5	Appoint Verifying Officer.....	22
3.6	Cancel Cards (DPC and DTC).....	24
3.7	Changing Credit Limits On Purchasing Cards (PC).....	26
3.8	Call Centre Operations.....	28
<b>4.</b>	<b>STANDARD OPERATING PROCEDURES .....</b>	<b>30</b>
4.1	Process Defence Travel Card (DTC) Applications .....	30
4.2	Daily Reconciliation of DINERS .....	32

<b>4.3</b>	<b>CMS Bank Reconciliation .....</b>	<b>33</b>
<b>4.4</b>	<b>Process and Review DPC Applications .....</b>	<b>34</b>
<b>4.5</b>	<b>Daily Reconciliation of NAB .....</b>	<b>35</b>
<b>4.6</b>	<b>Security of Data .....</b>	<b>36</b>
<b>4.7</b>	<b>CSO Potential Fraud/Misuse Reporting .....</b>	<b>37</b>
<b>4.8</b>	<b>Daily Reconciliation of ROMAN .....</b>	<b>38</b>
<b>4.9</b>	<b>Reporting Against DI(G)45-2 .....</b>	<b>39</b>
<b>4.12</b>	<b>Daily Reconciliation BORIS .....</b>	<b>42</b>
<b>4.13</b>	<b>Card Cancellation .....</b>	<b>44</b>
<b>4.14</b>	<b>Name Changes.....</b>	<b>46</b>
<b>4.16</b>	<b>DPC Limit Change .....</b>	<b>48</b>

## **1. Corporate Card Quality Assurance Manual**

### **1.1 Back Ground and Purpose**

Defence generally, the Finance Business Centre (FBC) and Corporate Card Support Centre (CCSC) specifically are responsible for the management of the Defence Corporate Card program including the Card Management System (CMS), Defence Purchasing Cards (DPC), and Defence Travel Cards (DTC). For the purposes of this document the terms DPC and DTC should be read to include the DMO Purchasing Card and DMO Travel Card.

The intent of this manual is to provide an annual review of the administrative processes around the CMS and Corporate Cards and identify an action plan going forward to address any risks as they arise.

### **1.2 Manual Scope**

The QA Processes outlined in this manual are the minimum expected as agreed by both FBC and CCSC. Any additional identified risks are to have processes put into place immediately to mitigate any possible ramifications and included in the next manual review.

### **1.3 Review Frequency**

Review of this manual is to be conducted in conjunction annually with the Business Continuity Plan with any new QA procedures or risks included in the manual at this time.

### **1.4 Manual Overview**

Part 2 of this document is to detail each of the QA tasks, their purpose, current status, issues, risks and resources required. Parts 3 & 4 provide the agreed Standard Operating Procedures as agreed by FBC and CCSC. The document provides the current status and ongoing SOP Requirement to ensure integrity of the CMS and allow for timely correction of anomalies.

### **1.5 Responsibility**

The Service Deliverer (CCSC) is responsible for the ongoing management of corporate card holders and associated data. It is important to note however that each card holder, their supervisors and groups more generally, also have a responsibility in the management of cards and associated data.

CCSC are to perform the QA tasks detailed below. These tasks are designed to identify potential issues with corporate card holders and associated data. Remedial action will depend on the results of the QA report and specific circumstances of the results.

CCSC are encouraged to refine delivery processes and to identify and pursue continuous improvement opportunities for best practice service delivery.

The Technical Authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).

Treasury and Banking within the CFO are also responsible for management of the NAB contract.

Integrated Travel Solutions (ITS) within, Non Equip Proc & Contract Branch DSRG, is responsible for Diners contract management.

## **2. Corporate Card Quality Assurance**

### **2.1 Corporate Card Quality Assurance Plan**

#### **CMS Users QA Overview**

Any member of Defence with a DRN account may obtain access to the CMS via a creation of a user ID. New CMS users are created via a self registration process. It is important to note that a CMS account, on initial creation does not really allow the user to do any more than log onto the system. It is not until actual cards, subordinates or special profiles are assigned that the account is able to actually 'do' anything. It is also important to note that in order to create a new user account an active Defence e-mail account is required.

A number of Users QAs have been devised;

- Review of new self registered users
- Review of CMS users with special profiles
  - Enterprise Controller
  - Admin Centre Controller / Super Admin Centre Controller
- Review contractor access to the CMS
- Active users not on PMKeyS CMS list
- Locked CMS Users with active Cards
- Locked Users with Unprocessed Transactions

#### **CMS Card QA Overview**

Access to a corporate card (DPC or DTC) is controlled through a card application process which determines the identity of the cardholder and entitlement to obtain a corporate card. The application process is not within the scope of this document. The focus of card QA is to ensure that data held (within the corporate management system CMS) on Defence Corporate cards is complete and accurate, and that the ongoing requirement for a card is reviewed when required.

A number of Card QAs have been devised;

- Cardholder not on PMKeyS CMS list
- Cardholder with more than 1 active card
- Review high limit cardholders
- Review contractors holding DPCs
- Review cardholders with both a Defence and DMO card
- Active cards not on ProMaster
- ProMaster record missing EID and/or e-mail details
- DPC Cash Withdrawal Access

## Executive summary of QA status and action items

QA	Risk
2.1.1 User - QA New Users Self Registered	Low
2.1.2 User - Enterprise Controller Report	Moderate
2.1.3 User – Admin Centre Controller Report	Low
2.1.4 User – Contractor Report	Low
2.1.5 User – Employee Users Not on PMKeys	Low
2.1.6 User – Locked Users with Active Cards	Low
2.1.7 User – Locked Users with Unprocessed Transactions	Low
2.1.8 Card – Active Cards Not on PMKeys	High
2.1.9 Card – More than One Active Card (Same Company Code)	Low
2.1.10 Card – High Limit Cards (>=\$250,000)	Moderate
2.1.11 Card – Report Group/Company Check	Low
2.1.12 Card – Missing EID or Email	Low
2.1.13 Card – Defence & DMO Card Holders - DTC	Low
2.1.14 Card – Defence & DMO Card Holders - DPC	Low
2.1.15 Card – Cards Not on Promaster	Low
2.1.16 Card – Cash Access Cards	Low

## QA Details

### 2.1.1 User - QA New Users (Self Registered)

The purpose of this review is to verify the details provided by the users during self registration matches data in the PMKeyS CMS File and that no other anomalies exist. A report is available within the CAPS system for this QA.

QA - Self Registered Users									
Users Created between: 1/1/08 and 31/1/08									
	Created	User ID	EID	Name	Email	Organisation	Supervisor		
<i>ProMaster:</i>	2/01/2008	BMADGE	8010729	Miss Bronwyn Madge	bronwyn.madge@defence.gov.au	EX_GID Governance and Implementation	LHIGGS		
<i>PMKeys:</i>	✓		8010729	Bronwyn Madge	bronwyn.madge@defence.gov.au	DS SC&G Deputy Secretary Strategy, Coordination and Gove			
<i>ProMaster:</i>	3/01/2008	CPHARRIS	8535428	Mr Christopher Harris	chris.harris@defence.gov.au	DM_LE A Land Engineering Agency	LDLANGEL		
<i>PMKeys:</i>	✓		8535428	Christopher Harris	Chris.HARRIS@defence.gov.au	DMO Land Systems Division			
<i>ProMaster:</i>	3/01/2008	DCLEE	8202950	SGT Daryl Lee	daryl.lee@defence.gov.au	AF_AIRFOR Air Force	SFGRIMME		
<i>PMKeys:</i>	✓		8202950	Daryl Lee	daryl.lee@defence.gov.au	AIR FORCE 44 Wing Detachment Tindal			
<i>ProMaster:</i>	4/01/2008	KMRAYMO1	8535917	Miss Kim Raymond	kim.raymond@defence.gov.au	DM_E&WSD Electronic & Weapons Systems	DAMITCH3		
<i>PMKeys:</i>	✓		8535917	Kim Raymond	Kim.RAYMOND@defence.gov.au	DMO Battlespace Communications SPO			
<i>ProMaster:</i>	4/01/2008	LMMURRAY	8012665	Ms Lesley Murray	lesley.murray@defence.gov.au	CS_PS Personnel Administration Branch	MJMCALIS		
<i>PMKeys:</i>	✓		8012665	Lesley Murray	lesley.murray@defence.gov.au	DEFSPS Personnel Services Division			
<i>ProMaster:</i>	4/01/2008	MEMELLOR	8011903	Ms Mary-Anne Mellor	mary-anne.mellor@defence.gov.au	COMPANY Dept. of Defence	LASPINA		
<i>PMKeys:</i>	✗		8011903	Mary-Anne Mellor	mary-anne.mellor@defence.gov.au	DS SC&G Deputy Secretary Strategy, Coordination and Gove			

## Risk Assessment

The risk associated with this QA task is **low**. A user account on its own does not allow the user to undertake transactions. The e-mail of the creator creates a direct link to the person who created the account.

## Frequency

CCSC are to review new users on a **weekly** basis.

## Status

This QA task has been completed in accordance with the SOP and is up to date as at release date.

**Agreed action plan**

Where a discrepancy is highlighted in the CAPS file CCSC are to investigate and as required update the ProMaster User account with the correct details. If the user is unresponsive or unable to be contacted the User account should be de-activated until details are able to be verified.

### **2.1.2 User - Enterprise Controller Report**

The purpose of this review is to ensure users holding the 'Enterprise Controller (EC)' profile are regularly reviewed and that where a user no longer requires the access it is promptly removed.

The EC access is the most powerful CMS profile with the ability to amend user and card details.

EC access can only be granted by another Enterprise Controller.

All Changes to Users and Accounts are logged by the CMS.

This profile must only be granted to members of the CCSC or FBC. It is important to note that even ECs cannot modify transaction details.

This QA task involves producing a report of all CMS users holding the EC Profile and having that list authorised by the Manager of the CCSC.

#### **Risk Assessment**

As Enterprise Controller is the most powerful CMS profile it should be held only by those who require it to undertake their duties as CMS administrators. The risks associated with inappropriate access to this role are **moderate**.

#### **Frequency**

The Manager of the CCSC should ensure Enterprise Controller access is removed at the time CCSC staff leave the area.

This QA task must be performed **monthly** and will ensure that where access has not immediately been removed on departure it does not go unnoticed.

#### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

#### **Agreed action plan**

Continue as per the SOP.

### **2.1.3 User - Admin Centre Controller Report**

The purpose of this review is to ensure users holding the 'Admin Centre Controller (ACC)' or 'Super Admin Centre Controller (SACC)' profile are regularly reviewed and where a user no longer requires the access it is removed.

The ACC profile allows the holder to monitor and report on the CMS activities of other CMS users. It is usually assigned for specific organisational units, for example Army. The ACC profile does not allow **any** updates.

The SACC profile has the rights of the ACC (as described above) plus the ability to update basic user contact details (those available to the user via self service). The SACC profile is allocated to group administrators who assist at the group level with the management of CMS users. Where an SACC makes an update it is logged in the audit trail.

ACC and SACC access can only be granted by an Enterprise Controller.

This QA task involves producing a report of all CMS users holding the ACC or SACC Profile and seeking from those users confirmation that ongoing access is required.

#### **Risk Assessment**

There is very little risk associated with ACC as it has no update ability whatsoever. SACC access does allow very limited update access to user contact details but does not allow any transaction processing, as such it is also considered a **low** risk.

### Frequency

Reconfirmation of all ACC/SACC access should occur **annually**.

### Status

This QA task has been completed in accordance with the SOP and is up to date as at release date.

### Agreed action plan

Continue as per the SOP.

#### 2.1.4 User - Contractor Report

The purpose of this review is to ensure contractor access to the CMS is removed when it is no longer required.

When a Contractor is granted access to the system the expiry date of their contract is recorded on the user profile.

Display Language	ENGLISH	▼
Post Code	2619	
Contractor Expiry	300608	
Phone 3		

This QA task involves producing a list of active contractor users and their contract expiry date. Where the expiry date has been exceeded the user must be contacted and an e-mail sent to CCSC advising of the new expiry date or confirmation the user account is to be locked. The e-mail should come from the contractors sponsor. Where no response is received the account shall be locked.

### Risk Assessment

The risk associated with ongoing access by contractors is considered **low**. Where a contractor has left the Department access to the DRN will also be removed. Without DRN access the contractor would not be able to access the CMS even if they have a current CMS account.

### Frequency

This QA task is to be undertaken **6 monthly**.

### Status

This QA task has been completed in accordance with the SOP and is up to date as at release date.

### Agreed action plan

Continue as per the SOP.

#### 2.1.5 User - Employee Users Not on PMKeys

The purpose of this review is to identify employee CMS users who **may** have left the Department and should have their access to the CMS revoked. The QA report matches EID on the CMS user profile versus the EID on the PMKeyS supplied data file. The QA report also provides a range of indicators such as whether the user has active cards, unprocessed transactions, when the account was created, when the user last logged on etc.

### Risk Assessment

The risk associated with active system users, where the employee has left Defence is **low**. Employees who leave the Department will lose access to the DRN (and Defence offices, through which it must be accessed) and as a consequence have no means of accessing the CMS.



### **Frequency**

This QA task should be undertaken **monthly**.

### **Status**

There are a number of issues associated with this task. The most important point to note is that the mere existence of a user on this QA report does not guarantee that the person is no longer with Defence. The employee file received by the CCSC for QA purposes does not contain all 'active' employees. It is therefore possible that an employee on this QA list does have an ongoing entitlement and need to access the system. Known groups of employees not on the PMKeyS list includes Foreign Military Personnel (exchange officers), and 'active' Reservists.

This QA task has been completed in accordance with the SOP and is up to date as at release date.

### **Agreed action plan**

Continue as per SOP

#### **2.1.6 User - Locked Users with Active Cards**

The purpose of this review is to identify CMS accounts which are locked and yet they have active cards assigned to those accounts. This situation is incompatible as a locked user cannot process transactions. To resolve the situation one of the following must occur;

- the user accounts must be reactivated, or
- the active card must be transferred to an active Account Holder, or
- the card must be cancelled.

The appropriate course of action will depend on the circumstances.

### **Risk Assessment**

The risk associated with this situation is **low**.

### **Frequency**

This QA Task is to be reviewed 6 **monthly**.

### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

### **Agreed action plan**

Continue as per the SOP.

#### **2.1.7 User - Locked Users with Unprocessed Transactions**

The purpose of this review is to identify CMS accounts which are locked and yet they have unprocessed transactions. This situation is of concern as if the user is locked the transactions are likely to remain unprocessed. To resolve the situation one of the following must occur;

- the user accounts must be reactivated, or
- the card with unprocessed transactions must be transferred to an active Account Holder, or
- an alternate user must be assigned authority to process the transactions.

The appropriate course of action will depend on the circumstances.

It should be noted that the responsibility for processing these transactions rests with the individual units and groups and these transactions will also show in the groups unprocessed transaction reporting (particularly once they become aged). Transaction processing or follow up is **not** a responsibility of the CCSC or FBC.

### **Risk Assessment**

The risk associated with this situation is **moderate**. It is important that transactions are processed as soon as possible as the older an unprocessed transaction becomes the greater the likelihood of difficulty obtaining the appropriate paperwork etc..

**Frequency**

This QA Task is to be reviewed **monthly**.

**Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

**Agreed action plan**

Continue as per the SOP.

**2.1.8 Card - Active cards not on PMKeyS**

The purpose of this review is to identify employee CMS users who **may** have left the Department and should have their DPC or DTC cancelled. The QA report matches EID on the CMS card profile versus the EID on the PMKeyS supplied data file.

**Risk Assessment**

The risk associated with ex-employees retaining active cards is **high**.

**Frequency**

This QA Task is to be reviewed **monthly**.

**Status**

There are a number of issues associated with this task. The most important point to note is that the mere existence of a user on this QA report does not guarantee that the person is no longer with Defence. The employee file received by the CCSC for QA purposes does not contain all 'active' employees. It is therefore possible that an employee on this QA list does have an ongoing entitlement and need to access the system. Known groups of employees not on the PMKeyS list includes Foreign Military Personnel (exchange officers), and 'active' Reservists.

This QA task has been completed in accordance with the SOP and is up to date as at release date.

**Agreed action plan**

Continue as per SOP

**2.1.9 Card – More than One Active Card (Same Company Code)**

The purpose of this review is to identify cardholders who have more than 1 active card (not including those who have a Defence card and a DMO card).

An individual may only have more than 1 DTC when approved by the Defence Contract Manager for the DTC Contract (Defence Travel Management)

An individual may have more than 1 DPC where a 'specified purpose' card is required. The most common example is where a card is issued for the purposes of 'currency flying' and a second is required as a unit purchasing card.

**Risk Assessment**

The risk associated with this situation is **low**. Each card will be subject to the processes and controls of the CMS and the 'plastic' used to undertake the transaction has little bearing. The cardholder does however, have access to the combined credit limit of the two cards.

**Frequency**

This QA Task is to be reviewed **monthly**.

Where the CCSC does not have a record of approval for a second card, the CCSC is to contact each of the duplicate holders seeking a business case for a second card and approval. Where the second card is not required (or in some cases lost or destroyed by the cardholder) it is to be cancelled.

Approval for a second card is to be reviewed **annually**. An updated business case must be supplied to support continued the need for more multiple cards.

#### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

#### **Agreed action plan**

CCSC to maintain records of cardholders authorised for more than 1 card and review annually.

CCSC to check for new duplicates monthly.

#### **2.1.10 Card – High Limit Cards (>=\$250,000)**

High limit cards are those corporate cards with a limit of \$250,000 or greater. This QA is to report on those cards and ensure there is ongoing justification for the high limit.

Note: The manager of the CCSC is authorised to approve high limit cards, on the basis the request has come from a Defence / DMO manager of an appropriate level who is not the cardholder, and the case for the high limit is a reasonable one.

#### **Risk Assessment**

The risk associated with high limit cards is **moderate** as the high limits are granted only if justified by a business requirement. Defence agreed however that the perceived risks associated with these cards justifies ongoing review and justification of limits.

#### **Frequency**

High limit cards and justification for the higher limit are to be reviewed **annually**.

#### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

#### **Agreed action plan**

CCSC to obtain justification of all high limit cards, and ensure all future high limits are justified, and reconfirmed annually.

#### **2.1.11 Card – Report Group/Company Check**

These QA tasks are designed to pick up anomalies on cards / ProMaster in relation to the company code. Such anomalies would indicate an error within the ProMaster data and / or and error by the card provider. For example if a DTC is in the diners Report Group 00034768 then the ProMaster company code must be 4100.

#### **Risk Assessment**

The risk associated with these errors are **low**, however if transactions are processed against the incorrect company code or if the anomalies are not corrected it may result in reconciliation issues

#### **Frequency**

This QA Task is to be undertaken **weekly** by the CCSC and inconsistencies addressed within 7 days.

#### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

**Agreed action plan**

Continue as per the SOP.

**2.1.12 Card – Missing EID or Email**

All cards should have an EID (or ODS for contractors) and an e-mail address. This QA identifies any that do not.

**Risk Assessment**

The risk associated with this situation is **Low**. The EID is an important field which enables other important validations, and uniquely identifies the individual cardholder.

**Frequency**

This QA Task is to be undertaken **monthly**.

**Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

**Agreed action plan**

Continue as per the SOP.

**2.1.13 Card – Defence and DMO Card Holders - DTC**

All Travel cards are issued as DMO or Defence cards, and transactions undertaken on that card can only be posted to the organisation to which the card belongs, which is generally the agency for which the person is employed or seconded. In most circumstances a person may only hold a travel card for a single agency, however in some cases a person may be approved to hold a card for each organisation. Examples include graduates who may be temporarily in DMO but should retain their Defence card for graduate program funded travel. Staff who holds a DTC for APS and for Reserve travel may be granted a second card if they can justify a minimum of 6 business trips per year.

This QA report identifies those personnel holding a Defence and DMO travel card. The list is to be reviewed for new entries and existing entries are to be confirmed annually.

It is agreed that a minimum of 6 trips per company code per year constitutes a business requirement to hold a card in both company codes.

**Risk Assessment**

The risk associated with this situation is **low**.

**Frequency**

This QA Task is to be performed **monthly** and authorised dual cardholders are to be confirmed annually.

**Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

**Agreed action plan**

Continue as per the SOP.

**2.1.14 Card – Defence and DMO Card Holders - DPC**

All purchasing cards are issued as DMO or Defence cards, and transactions undertaken on that card can only be posted to the organisation to which the card belongs, which is generally the agency for which the person is employed or seconded. In most circumstances a person may only hold a card for a single agency, however in some cases a person may be approved to hold a card for each organisation. Examples include DSG procurement staff who may be

authorised to hold a DMO DPC to make purchases on DMOs behalf. In all cases approval is required to concurrently hold a Defence and DMO card.

This QA report identifies those personnel holding a Defence and DMO Purchasing card. The list is to be reviewed for new entries and existing entries are to be confirmed annually.

#### **Risk Assessment**

The risk associated with this situation is **low**.

#### **Frequency**

This QA Task is to be performed **quarterly** and authorised dual cardholders are to be confirmed annually.

#### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

#### **Agreed action plan**

Continue as per the SOP.

#### **2.1.15 Card - Cards not on ProMaster**

All cards should be loaded onto ProMaster as soon as practicable after card creation (which may be the result of a new application or a replacement of a lost, stolen or damaged card). This QA identifies those cards which at the time of the report have not been loaded.

#### **Risk Assessment**

The risk associated with this situation is **low**. As soon as a card not on ProMaster has a transaction it will result in an 'unprocessed transaction' on CMS, which in turn will prompt the CCSC to identify and immediately load the card.

#### **Frequency**

This QA Task is to be reviewed **weekly**.

#### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

#### **Agreed action plan**

Continue as per the SOP.

#### **2.1.16 Card – Cash Access Cards**

All Purchasing Cards should issued without cash access. An initial business case must be submitted by the business area requesting cash access. Business areas are required to justify continued cash access twice a year. This QA identifies all purchasing cards that have cash access.

#### **Risk Assessment**

The risk associated with this situation is **low**. Card holders can only draw up to \$1,000 per day without prior arrangements. All cash withdrawals are still required to be acquitted with in the units & NAB have an exceptional fraud detection team that monitor cash withdrawals.

#### **Frequency**

This QA Task is to be reviewed **6 monthly**

#### **Status**

This QA task has been completed in accordance with the SOP and is up to date as at release date.

**Agreed action plan**

Continue as per the SOP.

## **2.2 Suspected Fraud or Misuse**

### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) in its role of managing the CMS system and call centre operations will on a daily basis have contact with many CMS users and their transactions. The CCSC may also be the contact point where users report any suspicious or inappropriate card usage. The CCSC is to ensure that instances of suspected fraud or inappropriate use, either reported to them or observed in their daily operations are appropriately handled in accordance with DI(G) 45-2.

### **POLICY**

Defence Instruction (General) 45-2  
Chief Executive Instructions Part 2.3 Defence Purchasing Card  
Chief Executive Instructions Part 2.3 DMO Purchasing Card

### **RESPONSIBILITY**

The Service Deliverer (CCSC) is responsible for the appropriate handling of suspected fraud or inappropriate use in accordance with DI(G) 45-2. It is important to note that the CCSC is not an investigative authority and as such is not responsible for a detailed assessment of individual cases, or for the ongoing management of cases.

The CCSC is *not* responsible for proactively scanning or looking for potentially fraudulent transactions.

Treasury and Banking within CFO are responsible for NAB contract management.

The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).

Integrated Travel Solutions (ITS) within NECP Branch, DSRG, is responsible for Diners contract management.

The card providers (NAB / Diners) are responsible for reporting to Defence any transactions appearing to be the result of 3<sup>rd</sup> party fraud, or which appear to be significantly outside the profile of a 'usual' transaction. Both providers employ sophisticated tools and techniques to identify such transactions.

Individual card holders and CMS account holders are responsible for identifying suspicious, unusual or unauthorised transactions.

### **TIMING**

The CCSC should advise the appropriate investigative unit within 5 days of identifying a potentially fraudulent transaction.

### **TOOLS**

The tools associated with this service are;  
CAPS  
ProMaster  
PMKeyS

### **PROCEDURE**

All CCSC staff are to be advised and given a basic understanding of signs of potential misuse or fraud. All staff in the CCSC should ensure that such signs, when encountered are reported to the appropriate CCSC staff member.

The CCSC are to ensure all instances raised are appropriately investigated within the limitations of their responsibility. Ordinarily this would be a simple prima facie assessment of the information at hand, by an appropriate staff member.

Where, on consideration the CCSC believe the situation warrants further investigation, the details of the incident must be recorded and passed on to the appropriate investigative authority.

The CCSC shall also consider appropriate actions required to limit any loss to the Commonwealth such as immediate cancellation or suspension of a corporate card.

In the case of potential 3<sup>rd</sup> party fraud notified by the cardholder or card provider, the CCSC shall act promptly to limit any loss to the Commonwealth. The manager, or assigned member of the CCSC may be contacted outside normal working hours by the card provider in the case of suspected 3<sup>rd</sup> party fraud or to query exceptionally large or unusual transactions.

#### **RETAIN RELEVANT INFORMATION**

CCSC should retain a record of cases of potential misuse or fraud.

#### **QUALITY AND COMPLIANCE**

This task is important for the ongoing integrity of the card programs. It is important these tasks are regularly undertaken in accordance with this SOP.

The service deliverer may be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect this service.



### **3. CMS System & Account Administration**

#### **3.1 CMS Systems Operations**

##### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) shall manage all routine operations of the CMS system. This involves maintaining schedules, loading data files, routine maintenance and responding to exceptions.

##### **RESPONSIBILITY**

The Service Deliverer (CCSC) is responsible for all routine operations of the CMS system.

Treasury and Banking within CFO are responsible for NAB contract management.

The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).

The technical Authority will liaise with the software developer (Inlogik), and the **Defence Computing Bureau** in relation to this responsibility. Further details on this aspect are contained in the CMS Service Support Manual.

The **Defence Computing Bureau** is responsible for the IT operating environment.

Integrated Travel Solutions (ITS) within, NECP Branch, DSRG, is responsible for Diners contract management.

##### **TOOLS**

The tools associated with this service are;

CAPS

ProMaster

PMKeyS

Incident Database

CMS Service Support Manual

## **PROCEDURE**

CCSC shall undertake the following routine operations of the CMS system.

Maintain and monitor the batch schedules of the CMS. The results of overnight processing must be checked daily (working days). All issues falling outside the normal operations must be recorded. Failures in the operating environment must be reported to the **DCB Incident Management Centre, Email: [imc@dcb.defence.gov.au](mailto:imc@dcb.defence.gov.au)**.

Receive and prepare for CMS processing card provider transaction files. Transaction files must be loaded within one business day of availability to CCSC.

Schedule monthly accrual activity and verify results. The accrual jobs are to be scheduled on the morning of the last business day of each month following the daily GL post activities. CCSC are to ensure no further GL post activities are run prior to the following month.

Verify the success of daily GL post activities, including successful processing by ROMAN. To be completed daily.

Manage transactions sent to ROMAN Batch Input sessions (these are the transactions that fail to post during the interface run). CCSC is to aim for completion of batch transactions within 5 days (noting this is not always possible due to dependence on external parties / system issues).

## **RETAIN RELEVANT INFORMATION**

CCSC shall retain a record of all reconciliation activities.

All system incidents outside of normal operations are to be recorded in the incident database.

## **QUALITY AND COMPLIANCE**

This task is a core activity of the CCSC. It is important these tasks are regularly undertaken in accordance with this SOP.

The service deliverer may be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect this product.

### 3.2 Process DTC Applications

#### SERVICE TO BE DELIVERED

The Service Deliverer (CCSC) is to provide a national service to Defence / DMO for the processing of Travel Card (DTC) applications. This involves the appropriate review of applications, maintaining controls and policy adherence, managing issues associated with application and liaising with the DTC issuing company (Diners). This service commences with the receipt of a DTC application and ends when the applicant has received their card and its details have been added to the ProMaster system.

#### POLICY

CEI 2.3 Defence Credit Cards  
FINMAN 5 – 2.3 Defence Credit Cards

#### RESPONSIBILITY

The Service Deliverer (CCSC) is responsible for the conduct of this task, and associated delivery methods and working level procedures (micro).

The Technical Authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).

Integrated Travel Solutions (ITS) within, NECP Branch, DSRG, is responsible for Diners contract management.

#### TIMING

DTC applications should be processed within 5 working days of receipt by the CCSC. In this context processing is deemed to have occurred either when the request for the card has been issued to Diners, or the applicant has been contacted and advised of an error or omission in their application, or that their application has been rejected.

#### TOOLS

The tools associated with this service are;

- CAPS
- PMKeyS
- DPC Application Forms (Web)
- CCSC Web Site
- FIND
- ProMaster Card Management System (CMS)

#### PROCEDURE

The service deliverer shall ensure that each card application is appropriately completed and verified. This includes:

- Ensure the applicant has provided all mandatory data for the processing of the application.
- Ensure applicant is a current employee of Defence.
- Verify the validity of the company code and cost centre on the application.
- Verify that the nominated account holder is a valid CMS user.
- Verify all other fields are completed with credible data.

For card applicants seeking a card limit greater than \$100,000 a business case from the supervisor of that applicant **must** be provided to the CCSC. The manager of the CCSC must endorse the business case for credit limits exceeding **\$100,000**.

DTCs must not be issued to contract personnel.

The Service Deliverer shall add the card to the ProMaster system within two weeks of the card creation date.

#### **RETAIN RELEVANT INFORMATION**

The service deliverer is to retain appropriate details in relation to each application;

- Diners New Application (NA) files (electronic).
- Business case for applicants seeking limits in excess of **\$100,000**.

#### **QUALITY AND COMPLIANCE**

This service has a high level of associated financial risk, and is subject to regular scrutiny by internal and external audit (ANAO). As such it must be undertaken to the highest standards and with appropriate risk management controls in place.

The service deliverer will regularly be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect the integrity or security of this service.

### **3.3 Process DPC Application**

#### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) is to provide a national service to Defence and DMO for the processing of Defence/DMO Purchasing Card (DPC) applications. This involves the appropriate review of applications, maintaining controls and policy adherence, managing issues associated with application and liaising with the DPC issuing company (NAB). This service commences with the receipt of a DPC application and ends when the applicant has received their card and its details have been added to the ProMaster system.

#### **POLICY**

Chief Executive Instructions Part 2.3 Defence Purchasing Card  
Chief Executive Instructions Part 2.3 DMO Purchasing Card

#### **RESPONSIBILITY**

The Service Deliverer (CCSC) is responsible for the conduct of this task, and associated delivery methods and working level procedures (micro).

**The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).**

**Integrated Travel Solutions (ITS) within NECP Branch, DSRG, is responsible for Diners contract management.**

#### **TIMING**

DPC applications should be processed within 5 working days of receipt by the CCSC. In this context processing is deemed to have occurred either when the request for the card has been made to the NAB, or the applicant has been contacted and advised of an error or omission in their application, or that their application has been rejected.

#### **TOOLS**

The tools associated with this service are;

- CAPS
- PMKeyS
- NAB Connect
- DPC Application Forms
- CCSC Web Site
- FIND
- ProMaster Card Management System (CMS)

#### **PROCEDURE**

The service deliverer shall ensure that each card application is appropriately completed and approved by the relevant person(s). This includes:

- Ensure the applicant has provided all mandatory data for the processing of the application.
- Ensure the application has been signed by a recognised Verifying Officer for the standard 100 point check. . The EID of the VO must also be recorded on the application form.
- Ensure the application has been signed by a recognised Authorising Officer for the provision of each card and its credit limit. The EID of the AO must also be recorded on the application form.
- Authorisation and detail (in the form of an e-mail or minute) from the supervisor of each applicant regarding the cost centre to be used against each card.
- Ensure applicant is a current employee of Defence / DMO, or refer to the note below relating to contractor applicants.
- Ensure the applicant has completed the purchasing card e-learning course.

For card applicants seeking a card limit greater than \$250,000 a business case from the supervisor of that applicant **must** be provided to the CCSC. The manager of the CCSC must endorse the business case for credit limits exceeding \$250,000.

For card applicants seeking cash access to be attached to their card a business case from the authorising officer and supervisor of that applicant **must** be included with their application.

Where the applicant is a contractor to Defence, the application **must** be accompanied by a business case endorsed by a Defence 'sponsor'. The business case must include details of the sponsor, including their EID (to be verified), the ODS identifier of the contractor, the requirement for the contractor to have a DPC and the contract expiry date. The sponsor **must** be advised of their responsibility to immediately advise the CCSC when the contractor engagement ceases with Defence or, when the card is no longer required by the contractor. The manager of the CCSC must endorse the business case for contractor applications.

The Service Deliverer shall add the card to the ProMaster system within two weeks of the card creation date.

#### **RETAIN RELEVANT INFORMATION**

The service deliverer is to retain appropriate details in relation to each application;

- A copy of the NAB application form.
- A copy of the AC101 – Cardholder acknowledgement
- A copy of the 100 point verification form.
- Business case for applicants seeking limits in excess of \$250,000.
- Business cases for applicants seeking cash access
- Business cases for contractors to hold a DPC

#### **QUALITY AND COMPLIANCE**

This service has a high level of associated financial risk, and is subject to regular scrutiny by internal and external audit (ANAO). As such it must be undertaken to the highest standards and with appropriate risk management controls in place.

The service deliverer will regularly be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect the integrity or security of this service.

### **3.4 Appoint Authorising Officer (NAB)**

#### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) is to provide a national service as Authorising Officers for the Defence Purchasing Card (DPC). Authorising Officers are empowered by the NAB to approve DPC applications and authorise administrative changes. This includes adding cardholders, cancelling cards and adjusting credit limits. This service commences with the receipt of an Authorising Officer application and ends when the applicant has received confirmation of their appointment or rejection of their application.

#### **POLICY**

Chief Executive Instructions Part 2.3 Defence Purchasing Card  
Chief Executive Instructions Part 2.3 DMO Purchasing Card

#### **RESPONSIBILITY**

The Service Deliverer (CCSC) is responsible for the conduct of this task, and associated delivery methods and working level procedures (micro).

**The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).**

**Integrated Travel Solutions (ITS) within NECP Branch, DSRG, is responsible for Diners contract management.**

#### **TIMING**

DPC applications should be processed within 5 working days of receipt by the CCSC. In this context processing is deemed to have occurred either when the request for the card has been made to the NAB, or the applicant has been contacted and advised of an error or omission in their application, or that their application has been rejected.

#### **TOOLS**

The tools associated with this service are;

- PMKeyS
- CCSC Web Site

#### **PROCEDURE**

The service deliverer shall ensure that each Authorising Officer is appropriately approved by the relevant person. The approval officer role is limited to:

- Manager CCSC
- Assistant Manager CCSC
- DPC Administrator

#### **RETAIN RELEVANT INFORMATION**

The role of Authorising Officer is limited to members of the CCSC only, a separate QA process is deemed unnecessary as the arrangements are in place with NAB to not accept card applications not approved by one of the 3 team members.

#### **QUALITY AND COMPLIANCE**

This service has a high level of associated financial risk, and is subject to regular scrutiny by internal and external audit (ANAO). As such it must be undertaken to the highest standards and with appropriate risk management controls in place.

The service deliverer will regularly be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect the integrity or security of this service.

### **3.5 Appoint Verifying Officer.**

#### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) is to provide a national service to Defence / DMO for the appointment of Verifying Officers for the Defence / DMO Purchasing Card (DPC). Verifying Officers are responsible for confirming the identification of all new cardholders to satisfy the Financial Transactions Reports Act requirements. This service commences with the receipt of a Verifying Officer application and ends when the applicant has received confirmation of their appointment or rejection of their application.

#### **POLICY**

Chief Executive Instructions Part 2.3 Defence Purchasing Card  
Chief Executive Instructions Part 2.3 DMO Purchasing Card

#### **RESPONSIBILITY**

The Service Deliverer (CCSC) is responsible for the conduct of this task, and associated delivery methods and working level procedures (micro). CCSC are encouraged to refine delivery processes and to identify and pursue continuous improvement opportunities for best practice service delivery.

**The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).**

#### **TIMING**

Verifying Officer applications should be processed within 10 working days of receipt by the CCSC. In this context processing is deemed to have occurred either when the applicant has received confirmation of their appointment or the applicant has been contacted and advised of an error or omission in their application, or that their application has been rejected.

#### **TOOLS**

The tools associated with this service are;  
VO Application Form  
PMKeyS  
CCSC Web Site  
FIND

#### **PROCEDURE**

The service deliverer shall ensure that each Verifying Officer application is appropriately completed and approved by the relevant person(s). This includes:

Ensure the applicant has provided all mandatory data for the processing of the application.  
Ensure applicant is a current employee of Defence. Contractors may not be appointed as Verifying Officers.  
Ensure the application has the approval of a registered Authorising Officer, and ensure the Authorising Officer is a current employee of Defence.

Completed applications must be signed by the Manager CCSC.

#### **RETAIN RELEVANT INFORMATION**

The service deliverer is to retain appropriate details in relation to each application;  
A copy of the completed application form as issued to the NAB.

The CCSC must retain a register of all current Verifying Officers.

Verifying Officers are to be reviewed at least once every 12 months. Personnel no longer requiring the role of Verifying Officer are to be removed from the register and the NAB advised that their authority has been revoked.

#### **QUALITY AND COMPLIANCE**



This service has a **low** level of associated financial risk, and is subject to regular scrutiny by internal and external audit (ANAO). As such it must be undertaken to the highest standards and with appropriate risk management controls in place.

The service deliverer will regularly be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect the integrity or security of this product.

### **3.6 Cancel Cards (DPC and DTC)**

#### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) is to provide a national service to Defence / DMO for the cancellation of corporate cards (DPC and DTC).

#### **POLICY**

Chief Executive Instructions Part 2.3 Defence Purchasing Card

Chief Executive Instructions Part 2.3 DMO Purchasing Card

#### **RESPONSIBILITY**

The primary responsibility for the cancellation of a corporate card when it is no longer required (either due to a change of role, or exit from Defence / DMO) rests with the cardholder, and should be ensured by their manager.

The Service Deliverer (CCSC) is responsible for verifying and actioning requests for card cancellation and associated delivery methods and working level procedures (micro).

**The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).**

**Integrated Travel Solutions (ITS) within NECP Branch, DSRG, is responsible for Diners contract management.**

#### **TIMING**

Requests for card cancellation should be processed within 5 working days of receipt by the CCSC.

#### **TOOLS**

The tools associated with this service are;

CAPS

PMKeyS

CCSC Web Site

FIND

#### **PROCEDURE**

The service deliverer shall action card cancellation requests. A request for cancellation may come from;

The actual cardholder

The cardholders current supervisor, or where the cardholder has left Defence

A Defence business manager or administrator (including CMS Admin Centre Controllers)

The CMS account holder for the card to be cancelled

**PmKeys file**

There must be sufficient information in the request to uniquely identify the card to be cancelled.

The requestor of the cancellation must be advised that arrangements are to be made to complete any unprocessed transactions or outstanding disputed items.

In the event the CCSC is the first point of contact after a card has been lost, stolen or has been fraudulently used (or suspected of fraudulent use) by a third party, the requestor must be advised to immediately contact the card provider (NAB or Diners).

#### **RETAIN RELEVANT INFORMATION**

For DTC cancellations, the reason for cancellation must be entered in the CAPS system.

#### **QUALITY AND COMPLIANCE**

It is important that cancellation requests are actioned in accordance with this SOP, as undue delays to cancellations may result in additional unwanted transactions being charged to the card (for example periodical charges).

It is also important that care is taken to ensure the correct card is cancelled. Cancellation of the incorrect card may result in inconvenience and additional work by a member whose card is incorrectly cancelled.

It is generally sufficient for the CCSC to accept a request for cancellation on face value, i.e. there is no need to verify the requestors details so long as the request has been received via a standard Defence email address.

The service deliverer may be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect the integrity or security of this product.

### **3.7 Changing Credit Limits On Purchasing Cards (PC)**

#### **BACKGROUND**

To reduce exposure towards potential fraud, each PC has an approved spending limit. Defence and DMO business units establish the approved card limit for each PC when issuing a card to a new account holder.

**GCFO's** and their business units are requested to review card limits annually too ensure that the spend limit of the PC is in accordance with business requirements.

#### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) is to provide a national service to Defence and DMO for the processing of Defence/DMO Purchasing Card (PC) for changes to spending limits. This involves the appropriate review of the Spending Limits form AD773, maintaining controls and policy adherence. This service commences with the receipt of the AD773 – Defence and / or DMO PC application and ends when the adjustments to the spending limit have been added.

#### **POLICY**

DPC, DTC and CMS User Manual

#### **RESPONSIBILITY**

The Service Deliverer (CCSC) is responsible for the conduct of this task, and associated delivery methods and working level procedures (micro). CCSC are encouraged to refine delivery processes and to identify and pursue continuous improvement opportunities for best practice service delivery.

**The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).**

#### **TIMING**

PC change in credit limits should be processed within 5 working days of receipt by the CCSC.

#### **TOOLS**

The tools associated with this service are;

CAPS

PMKeyS

NAB Connect

DPC Application Forms

CCSC Web Site

FIND

ProMaster Card Management System (CMS)

#### **PROCEDURE**

The service deliverer shall ensure that each card application is appropriately completed and approved by the relevant person(s). This includes:

Ensure the cardholder has provided all mandatory information for processing i.e. Card Holders details – family name, given names and employee ID, Card Details – last four digits of the card number, current card limit, proposed new card limit

Ensure there is sufficient information with regards to the justification for change to card limit  
Ensure the application has been signed by the Card Holder and the Supervisor with the EID.

Ensure the application is signed by a recognised Authorising Officer for the provision of its credit limit change. The EID of the AO must also be recorded on the change of limit form.

Ensure applicant is a current employee of Defence / DMO, or refer to the note below relating to contractor applicants.

For card applicants seeking a card limit change greater than \$250,000 a business case from the supervisor of that applicant **must** be provided to the CCSC. The manager of the CCSC must endorse the business case for credit limits exceeding \$250,000.

Where the applicant is a contractor to Defence, the application **must** be accompanied by a business case endorsed by a Defence 'sponsor'. The business case must include details of the sponsor, including their EID (to be verified), the ODS identifier of the contractor, the requirement for the contractor to have a change in credit limit for the PC and the contract expiry date. The sponsor **must** be advised of their responsibility to immediately advise the CCSC when the contractor engagement ceases with Defence or DMO, when the card is no longer required by the contractor. The manager of the CCSC must endorse the business case for contractor limits change.

The Service Deliverer shall adjust the card limit and will advise the customer within 3 days of the card creation date.

#### **QUALITY AND COMPLIANCE**

This service has a high level of associated financial risk, and is subject to regular scrutiny by internal and external audit (ANAO). As such it must be undertaken to the highest standards and with appropriate risk management controls in place.

The service deliverer will regularly be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect the integrity or security of this service.

### **3.8 Call Centre Operations**

#### **SERVICE TO BE DELIVERED**

The Service Deliverer (CCSC) shall provide a national call centre/help desk service Mon – Fri between 0830 – 1630 for all corporate card queries relating to the use of the Card Management System (CMS), as well as advice on obtaining either a Defence/DMO travel card or purchasing card. Service is delivered upon receipt of an email to the corporate cards email account or a telephone call to the 1800 007 606 number.

#### **POLICY**

Dependant upon the query received, reference all other SOP's for policy guidance.

#### **RESPONSIBILITY**

The Service Deliverer (CCSC) is responsible for all routine queries of the CMS system.

The technical authority (FBC) is responsible for ensuring the necessary delivery tools are available to support the process and maintaining the top level (macro) delivery process (this document).

The Technical Authority as system owner of the CMS is responsible for the ongoing technical maintenance of the CMS, in terms of fixes, upgrades and functional enhancements. The technical Authority will liaise with the software developer (Inlogik), and the **Defence Computing Bureau** in relation to this responsibility. Further details on this aspect are contained in the CMS Service Support Manual.

The **Defence Computing Bureau** is responsible for the IT operating environment.

**Integrated Travel Solutions (ITS) within NECP Branch, DSRG, is responsible for Diners contract management.**

.

#### **TIMING**

Telephone calls should be answered within 1.45.

Password resets should be actioned within 30 minutes.

All other emails to be answered in receipt date order.

#### **TOOLS**

The tools associated with this service are;

CAPS

ProMaster – updates to be placed on the privacy screen

PMKeyS

Incident Database

DTC DPC User Manual

Email

CCSC Website

#### **PROCEDURE**

CCSC shall undertake the following routine procedures for the operation of the call centre.

Provides administrative and helpdesk support to Defence Travel Card (DTC) holders and Purchasing Card (PC) holders in both Defence and the Defence Materiel Organisation (DMO).

Is the central coordination point for DTC & PC activity and liaises closely with the card providers (Diners/NAB) on card issue, re-issue, cancellation and credit limit activity.

Administers the Card Management System (CMS) and performs the required reconciliation and maintenance functions for the CMS.

Performs a quality assurance role and fraud detection/prevention role in consultation with the Inspector General Group.

Follow up on all calls received outside of business hours by checking the answering machine each morning.

**RETAIN RELEVANT INFORMATION**

CCSC shall retain all copies of emails actioned.

Manager CCSC is to monitor the number of emails actioned and calls received and report to **DFBC on a monthly basis.**

All system incidents outside of normal operations are to be recorded in the incident database and advise the CMS Technical Contractor.

**QUALITY AND COMPLIANCE**

This task is a core activity of the CCSC. It is important these tasks are regularly reviewed for consistency.

The service deliverer may be required to provide documentation, evidence and commentary to the TA and auditors in relation to this process.

The service deliverer must ensure that the TA is advised without delay of any issues or events which may affect this product.

## **4. Standard Operating Procedures**

### **4.1 Process Defence Travel Card (DTC) Applications**

#### **PURPOSE**

The purpose of this SOP is to ensure that DTC applications are appropriately reviewed and verified before a card is issued to the applicant.

#### **POLICY**

**DECA 2012 – 2014**

*H1.1 Employees will be provided with the facility to meet reasonable travel costs on the basis that they neither gain nor lose financially when required to travel on official business.*

#### **PACMAN Chapter 9, Part 5, Division 2**

*This Division applies to a member (including a member on Reserve service) who uses a travel card when they are required to travel on Defence business.*

#### **RESPONSIBILITY**

This task is to be undertaken by the Corporate Card Support Centre (CCSC)

#### **TIMING**

Applications should be processed within 5 working days of receipt by the CCSC.

#### **TOOLS**

- Electronic DTC application web page (Integrated Travel Solutions web site)
- Corporate.cards email Inbox
- CAPS System

#### **PROCEDURE**

1. Retrieve email application from [corporate.cards@defence.gov.au](mailto:corporate.cards@defence.gov.au)
2. Load application into CAPS
3. Verify and confirm application data (CAPS)
  - PMKeyS Match<sup>1</sup>
  - Applicant age<sup>2</sup>
  - Address must be a Defence work location
  - The email address must match the name of the applicant<sup>3</sup>
  - Valid Company code / Cost centre<sup>4 5</sup>
  - Nominated account holder is a valid CMS user

---

<sup>1</sup> CAPS matches application data with a regularly (no less than monthly) updated PMKeyS data file.

<sup>2</sup> CAPS will not allow an application to proceed for an applicant under 18 years of age.

<sup>3</sup> Where available on the PMKeyS file the email can also be cross referenced with the PMKeyS email address.

<sup>4</sup> Where the company code does not match the PMKeyS group of the applicant, the applicant should be requested to provide confirmation. The justification should be noted in the application notes field.

<sup>5</sup> The cost centre code validation is simply that the provided code appears to be a valid cost centre (e.g. it is 6 characters long). CAPS will alert the reviewer when the cost centre does not meet the attributes of a valid cost centre.



- All other fields should be checked for credible data
4. Release application to Diners

**RETAIN RELEVANT DOCUMENTATION**

The DTC application process is paperless.

Application details are retained electronically in the CAPS System and periodically archived to the CAPS Archive Database

**REFERENCE MATERIAL**

CAPS Operations Manual

## **4.2 Daily Reconciliation of DINERS**

### **PURPOSE**

The purpose of this SOP is to ensure that data imported into the Card Management System (CMS) from Diners is not corrupted and reconciles.

### **POLICY**

N/A

### **RESPONSIBILITY**

This task is to be undertaken by the QAO, Corporate Card Support Centre (CCSC)

### **TIMING**

This task is to be performed on a daily basis.

### **TOOLS**

- File imported from Diners
- Standalone
- USB
- CMS

### **PROCEDURE**

- Download file, sent by Diners, from standalone and transfer to USB.
- Check and verify that the data exported is complete and has successfully transferred.
- Import Diners data, from USB, into CMS using CITRIX
- Process file in CMS ensuring both the Statement File and Statement Data run successfully.

### **RETAIN RELEVANT DOCUMENTATION**

Master copies of the files are held in two locations. One is held in CITRIX and a backup is held in Objective - 02. Prod & Services/AADINERS

### **REFERENCE MATERIAL**

### **CONTACTS**

#### **DINERS**

Bruce Griffiths

#### **CMS**

Graham Bresnahan  
Consultant, Finance Business Centre

**Jim Phillis**

**Defence Computing Bureau**

[Incident.management@dcb.defence.gov.au](mailto:Incident.management@dcb.defence.gov.au)

### **4.3 CMS Bank Reconciliation**

#### **PURPOSE**

The purpose of this SOP is to reconcile the card provider (NAB / VISA) payments to ensure all associated transactions have been loaded to the CMS and the payment amount accords with those transactions.

#### **POLICY**

N/A.

#### **RESPONSIBILITY**

This task is to be undertaken by the Finance Business Centre

#### **TIMING**

This task is to be performed on a monthly basis.

#### **MATERIALS**

- NAB Bank Statement for prior month (Defence) - This is sent directly to CCSC
- NAB Bank Statement for prior month (DMO) - This is sent to director T&B DMO
- CITRIX / ProMaster Tools Access
- ProMaster Enterprise Controller Access
- Excel Spreadsheet - "Bank statement reconciliation.xls"
- Word Document - "Reconciliation screen dumps 20xx\_200yy.doc"
- ROMAN Access with Display access to companies 1000, 3000 and 4100

#### **PROCEDURE**

Complete Excel Spreadsheet - "Bank statement reconciliation.xls"

- a. Transfer the following figures from the NAB statements to the NAB worksheets (Defence and DMO)
  - i. Billing Cycle
  - ii. Opening Balance
  - iii. Payments
  - iv. Purchases
  - v. Interest + Charges
  - vi. In Disputed Transactions (Total)
  - vii. Sweep amount advised
- b. Using CITRIX / ProMaster Tools run the SQL (Copy and paste from the SQL worksheet) for NAB (Defence and DMO). Update the statement period dates before executing. Transfer the results to the spreadsheet.
  - i. Sum of transactions Loaded

## **4.4 Process and Review DPC Applications**

### **PURPOSE**

The purpose of this SOP is to ensure that DPC applications are appropriately reviewed and verified before a card is issued to the applicant.

### **POLICY**

Chief Executive Instructions Part 2.3 Defence Purchasing Card

Chief Executive Instructions Part 2.3 DMO Purchasing Card

### **RESPONSIBILITY**

This task is to be undertaken by the Corporate Card Support Centre (CCSC)

### **TIMING**

Applications should be processed within 5 working days of receipt by the CCSC.

### **TOOLS**

- Paper copy DPC application
- Corporate.cards email Inbox
- PMkeys
- NAB Connect

### **PROCEDURE**

1. Retrieve faxed or mailed application: fax 1800 007 607
2. Verify and confirm application data (PMkeys, AO & VO spreadsheet)
  - PMKeyS Match & confirmation of training complete
  - Address must be a Defence work location
  - The email address must match the name of the applicant
  - Valid Company code / Cost centre
  - Nominated account holder is a valid CMS user
  - Credit limit is entered
  - Cash access yes or no (if yes business case must be submitted)
  - All other fields should be checked for credible data
3. Load application into NAB Connect

### **RETAIN RELEVANT DOCUMENTATION**

Application

100 point check (if sent)

AC101 (if sent)

### **REFERENCE MATERIAL**

<http://intranet.defence.gov.au/Finance/sites/CCSC/>  
Applying for a Defence Purchasing Card

## **4.5 Daily Reconciliation of NAB**

### **PURPOSE**

The purpose of this SOP is to ensure that data imported into the Card Management System (CMS) from NAB is not corrupted and reconciles.

### **POLICY**

N/A

### **RESPONSIBILITY**

This task is to be undertaken by the Assistant Manager, Corporate Card Support Centre (CCSC)

### **TIMING**

This task is to be performed on a daily basis.

### **TOOLS**

- Files imported from National Australia Bank (NAB)
- USB
- Standalone
- CMS

### **PROCEDURE**

- Download file, sent by NAB, from standalone and copy onto USB.
- Check and verify that the data exported is complete and has successfully transferred
- Import NAB data, from USB into CMS using the 'Upload Files' function in Activity Parameters.
- Process file in CMS ensuring both the DMO and Defence Statement File and Statement Data run successfully.

### **RETAIN RELEVANT DOCUMENTATION**

Master copies of the files are held in two locations. One is held in CITRIX and a backup is held in Objective – 02. Prod & Services /AANAB

### **REFERENCE MATERIAL**

### **CONTACTS**

#### **NAB**

PCard Support

#### **CMS**

Graham Bresnahan  
Consultant, Finance Business Centre

#### **Jim Phillis**

Defence Computing Bureau

[Incident.management@dcb.defence.gov.au](mailto:Incident.management@dcb.defence.gov.au)

## **4.6 Security of Data**

### **PURPOSE**

The purpose of this SOP is to ensure that all data pertaining to the Corporate Card Support Centre (CCSC) is kept secure and that user access is monitored on a regular basis.

### **POLICY**

### **RESPONSIBILITY**

This task is to be undertaken by the Assistant Manager (AM), CCSC

### **TIMING**

This task is to be performed on a daily basis.

### **TOOLS**

- Standalone
- CMS
- CITRIX
- Objective (DRMS)
- ROMAN
- BORIS
- [Corporate.cards@defence.gov.au](mailto:Corporate.cards@defence.gov.au)

### **PROCEDURE**

Data being exported to Diners must be encrypted.

Ensure that ALL CMS Users have access at the relevant level

Access to Objective is restricted to CCSC and FBC Staff

Access to Fraud is restricted to CCSCM, CCSCAM and CCSCCTL

Access to outlook email is restricted to CCSC staff

### **RETAIN RELEVANT DOCUMENTATION**

CCSC to retain relevant documentation.

### **REFERENCE MATERIAL**

### **CONTACTS**

#### **CIVILIAN**

Inspector Generals Department

[IG.Investigations@defence.gov.au](mailto:IG.Investigations@defence.gov.au)

#### **SERVICE**

Aust. Defence Force Investigative Service

PM ADF (Global Address List)

#### **4.7 CSO Potential Fraud/Misuse Reporting**

##### **PURPOSE**

The purpose of this SOP is to ensure that all potential fraud/misuse of the Defence Travel Card (DTC) and/or Defence Purchasing Card (DPC) is reported and escalated to the relevant areas.

##### **POLICY**

- DI(G)45-2 Reporting and Investigation of Alleged Offences with the Australian Defence Organisation
- Chief Executive Instruction (CEI 3.3 Loss of Public Monies)
- Public Service Act 1999
- Defence Force Discipline Act 1982
- Criminal Code Act 1995
- Administrative Appeals Tribunal Act 1975

##### **RESPONSIBILITY**

This task is to be undertaken by all members of the CCSC.

##### **TIMING**

This task is to be performed and assessed with each customer contact made.

##### **TOOLS**

- CMS
- Corporate Card inbox
- 1800 007606 CCSC help desk

##### **PROCEDURE**

- Access customer records in CMS as per standard operating procedures.
- View transaction history details in CMS to determine activities on the account.
- Complete Potential Fraud Claim form, completing as much detail as possible including "quotes" from the caller/customer to assist with further investigation.
- If applicable, request that email be forwarded to [corporate.cards@defence.gov.au](mailto:corporate.cards@defence.gov.au) for cancellation of the card.
- Advise caller/customer that the unusual activity on the card must be reported IAW DI(G)45-2 and forward completed Potential Fraud Claim Form plus any other relevant documentation including emails and transaction history printout to the CCSCAM .

##### **RETAIN RELEVANT DOCUMENTATION**

All relevant documentation to be maintained by CCSCAM

##### **REFERENCE MATERIAL**

- DI(G)45-2 Reporting and Investigation of Alleged Offences with the Australian Defence Organisation
- Chief Executive Instruction (CEI 3.3 Loss of Public Monies)
- Public Service Act 1999
- Defence Force Discipline Act 1982
- Criminal Code Act 1995
- Administrative Appeals Tribunal Act 1975
- CMS User Manual

##### **CONTACTS**

###### **CIVILIAN**

Inspector Generals Department  
[IG.Investigations@defence.gov.au](mailto:IG.Investigations@defence.gov.au)

###### **SERVICE**

Aust. Defence Force Investigative Service  
PM ADF (Global Address List)

#### **4.8 Daily Reconciliation of ROMAN**

##### **PURPOSE**

The purpose of this SOP is to ensure that expenses data in the Card Management System (CMS) exports successfully and reconciles in ROMAN.

##### **POLICY**

N/A

##### **RESPONSIBILITY**

This task is to be undertaken by the AM, Corporate Card Support Centre (CCSC)

##### **TIMING**

This task is to be performed on a daily basis.

##### **TOOLS**

- CMS
- ROMAN

##### **PROCEDURE**

- Check and record posted ROMAN activity detailing transaction number and total value including BDC errors
- Check and record CMS activity detailing transaction number and total value and noting Gazettal File detail and Log ID.
- Above dot points must reconcile.
- If CMS and ROMAN do not balance check that the file in ROMAN ran successfully.
- Check the CMS scheduled activity process completed successfully.

##### **RETAIN RELEVANT DOCUMENTATION**

- Electronic Reconciliation recorded in 01. Reference Material/Reconciliations/Daily Reconciliations
- ROMAN
- CMS Activity Log

##### **REFERENCE MATERIAL**

##### **CONTACTS**

###### **ROMAN**

[CIOFS.customersupport@defence.gov.au](mailto:CIOFS.customersupport@defence.gov.au)

###### **CMS**

Graham Bresnahan  
Consultant, Finance Business Centre

###### **Jim Phillis**

Defence Computing Bureau

[Incident.management@dcb.defence.gov.au](mailto:Incident.management@dcb.defence.gov.au)



#### **4.9 Reporting Against DI(G)45-2**

##### **PURPOSE**

The purpose of this SOP is to ensure that data in the Card Management System (CMS), is checked for any transactional anomalies.

##### **POLICY**

- **DI(G)45-2 Reporting and Investigation of Alleged Offences with the Australian Defence Organisation**
- **Chief Executive Instruction (CEI 3.3 Loss of Public Monies)**
- **Public Service Act 1999**
- **Defence Force Discipline Act 1982**
- **Criminal Code Act 1995**
- **Administrative Appeals Tribunal Act 1975**

##### **RESPONSIBILITY**

This task is to be undertaken by the CCSCAM

##### **TIMING**

This task is to be performed on a daily basis.

##### **TOOLS**

- CMS
- BORIS
- 1800 007 607

##### **PROCEDURE**

1. Check that all transactional data is within expected spend patterns.
2. Check that merchants are relevant to Defence requirements
3. Identify and contact relevant person in unit to verify transactions/spend
4. Report relevant findings to ADFIS, for Service members, and Inspector Generals Department, for Civilian members.

##### **RETAIN RELEVANT DOCUMENTATION**

All documentation is retained electronically in Objective – 02. Prod & Services/Potential Misuse/Customer Files

##### **REFERENCE MATERIAL**

##### **CONTACTS**

###### **CIVILIAN**

Inspector Generals Department  
IG.Investigations@defence.gov.au

###### **SERVICE**

Aust. Defence Force Investigative Service  
PM ADF (Global Address List)

###### **DINERS**

Bruce Griffiths

###### **NAB**

Sam Barnes

#### **4.11 DPC Cash Withdrawal Access**

##### **PURPOSE**

The purpose of this SOP is to ensure that access to withdraw cash on DPC's are monitored only given where necessary.

##### **POLICY**

Chief Executive Instructions Part 2.3 Defence Purchasing Card  
Chief Executive Instructions Part 2.3 DMO Purchasing Card

##### **RESPONSIBILITY**

This task is to be undertaken by Corporate Card Support Centre (CCSC)

##### **TIMING**

This task must be done on a bi-annual (Twice yearly) basis.

##### **TOOLS**

- CAPS
- Files imported from NAB

##### **PROCEDURE**

- AM CCSC to provide a list of all cards with Cash Access
- Emails to be sent to all card holders requesting that they provide a justification as to the need for cash withdrawal access
- Justification is reviewed and emails kept for future reference.

##### **RETAIN RELEVANT DOCUMENTATION**

CCSC to retain relevant documentation

##### **REFERENCE MATERIAL**

##### **CONTACTS**

#### **4.10 Daily Reconciliation of CMS**

##### **PURPOSE**

The purpose of this SOP is to ensure that data imported into the Card Management System (CMS) is not corrupted and reconciles.

##### **POLICY**

N/A

##### **RESPONSIBILITY**

This task is to be undertaken by the AM, Corporate Card Support Centre (CCSC)

##### **TIMING**

This task is to be performed on a daily basis.

##### **TOOLS**

- CMS
- File imported from Diners
- Files imported from NAB
- ROMAN
- BORIS

##### **PROCEDURE**

- Check and verify that all imported files from DINERS and NAB are complete.
- Import all files into CMS and confirm all have run successfully.
- Check and confirm ROMAN has received all exported posted CMS data
- Check and confirm BORIS has received all expense and transactional data

**RETAIN RELEVANT DOCUMENTATION**

**REFERENCE MATERIAL**

**CONTACTS**

**CMS**

Graham Bresnahan  
Consultant, Finance Business Centre

**NAB**

PCard Support  
[pcardsupport@national.com.au](mailto:pcardsupport@national.com.au)

#### **4.12 Daily Reconciliation BORIS**

##### **PURPOSE**

The purpose of this SOP is to ensure that Expense and Transactional data in the Card Management System (CMS) reconciles in BORIS.

##### **POLICY**

N/A

##### **RESPONSIBILITY**

This task is to be undertaken by the Corporate Card Support Centre (CCSC)

##### **TIMING**

This task is to be performed on a daily basis.

##### **TOOLS**

- CMS
- BORIS

##### **PROCEDURE**

1. Create four 'Ad Hoc Report' reports in BORIS setting parameters for Card Type, Unit ID Hierarchy and Statement Date.
  - **VISA** Reconciliation – Transactions
  - **DINERS** Reconciliation – Transactions
  - **VISA** Reconciliation – Expenses
  - **DINERS** Reconciliation – Expenses
2. Reconcile transactions in CMS and BORIS.
3. Any discrepancies that appear in BORIS must be reported.

##### **RETAIN RELEVANT DOCUMENTATION**

Electronic Reconciliation recorded in 02. Prod & Services/Reconciliations

##### **REFERENCE MATERIAL**

##### **CONTACTS**

##### **BORIS**

#### **4.10 Daily Reconciliation of CMS**

##### **PURPOSE**

The purpose of this SOP is to ensure that data imported into the Card Management System (CMS) is not corrupted and reconciles.

##### **POLICY**

N/A

##### **RESPONSIBILITY**

This task is to be undertaken by the AM, Corporate Card Support Centre (CCSC)

##### **TIMING**

This task is to be performed on a daily basis.

##### **TOOLS**

- CMS
- File imported from Diners
- Files imported from NAB
- ROMAN
- BORIS

##### **PROCEDURE**

- Check and verify that all imported files from DINERS and NAB are complete.
- Import all files into CMS and confirm all have run successfully.
- Check and confirm ROMAN has received all exported posted CMS data
- Check and confirm BORIS has received all expense and transactional data

#### **RETAIN RELEVANT DOCUMENTATION**

#### **REFERENCE MATERIAL**

#### **CONTACTS**

##### **CMS**

Graham Bresnahan  
Consultant, Finance Business Centre  
(

##### **CMS**

Troy Larke  
Business Operations Manager,  
Campbell Park ACT

##### **Jim Phillis**

**Defence Computing Bureau**

[Incident.management@dcb.defence.gov.au](mailto:Incident.management@dcb.defence.gov.au)

## **4.13 Card Cancellation**

### **PURPOSE**

The purpose of this SOP is to outline the procedure for cancellation of DTC and DPC cards.

### **RESPONSIBILITY**

This procedure applies to all members of CCSC.

### **TIMING**

The procedure is to be followed in response to all valid requests for a card cancellation.

### **TOOLS**

- CMS
- CAPS
- NAB Connect
- PMKeyS

### **PROCEDURE**

- Review request for cancellation
  - The card to be cancelled must be able to be distinguished from other cards (and users) with a combination of the following details:
    - Cardholders Name
    - PMKeyS
    - Last 4 digits on the card
    - Email Address
    - CMS User ID
    - Card Type and Organisation (Defence/DMO)
  - If there has not been enough supplied information to sufficiently determine the correct card to cancel, a return message must be sent to request the required information.
  - PMKeyS can be used to confirm that a member no longer has need of the card in cases where the cancellation is requested from someone other than the cardholder and the reason is for discharge/separation or retirement from the department.
- Check for CMS Transactions
  - If there are transactions still outstanding on the card, inform the requesting member but proceed with the cancellation.
- Cancel the card
  - DTC
    - Card cancellations should be done in CAPS where possible. Email date and name of the CCSC member who cancelled the card should be entered in the notes field.
    - Where CAPS is unavailable, cancellation can be actioned through an email sent to Diners Club.
  - DPC
    - Card cancellations should be done in NAB Connect, unless a member with access to NAB Connect is unavailable.
    - If cancellation cannot be done in NAB Connect, cancellation can be actioned through sending an email to the bank, NAB.
- Lost/Stolen Cards
  - If a card has been lost or stolen, a copy of the message must be saved in the DPC Support – Quality Analysis Jobs – Lost or Stolen Cards folder.
- Confirm Action
  - Send a return message to the requesting member informing them of the cancellation and advising them to ensure that the card has been cancelled.

### **RETAIN RELEVANT DOCUMENTATION:**

The request will be accepted by email only. All emails to be retained by CCSC.

**CONTACTS:**

**CCSC**

Phone: 1800 007 606

Email: [corporate.cards@defence.gov.au](mailto:corporate.cards@defence.gov.au)

#### **4.14 Name Changes**

##### **PURPOSE**

The purpose of this SOP is to ensure that customers have cards and CMS accts that reflect their name after a name change

##### **POLICY**

##### **RESPONSIBILITY**

This task is to be undertaken by Customer Support Officers of the CCSC.

##### **TIMING**

This task is to be performed on an as required basis.

##### **TOOLS**

- CMS
- Corporate Card inbox
- PMKeys
- CAPS
- NAB Connect

##### **PROCEDURE**

- Access customer records in CMS as per standard operating procedures.
- Ensure that PMKeys reflects the name change of the member .
- Contact card provider by either email or automated system (NAB connect/CAPS) to arrange issue of new card.
- Create new userid in CMS reflecting new name.
- Transfer all subordinates and acct holder cards to the newly created profile.
- Render old acct "inactive" in CMS

##### **RETAIN RELEVANT DOCUMENTATION**

The request will be accepted by email only. All emails to be retained by CCSC.

##### **REFERENCE MATERIAL**

- DPT DTC and CMS User Manual

##### **CONTACTS**

Diners 1800 105660    defence@diners.com.au

NAB    131012 pcardsupport@national.com.au



#### **4.15 Resetting a password from an Email request**

##### **PURPOSE**

The purpose of this SOP is to outline the standard procedure for resetting a CMS Password from an email.

##### **RESPONSIBILITY**

This procedure applies to all members of CCSC.

##### **TIMING**

The procedure is to be followed in response to all email requests for a password reset.

##### **TOOLS**

- Emailed Password Request
- CMS

##### **PROCEDURE**

- Review data within the received email:
  - The information in the email must be enough to distinguish the member requiring a password reset from other users. The information used to identify the user should include as a minimum:
    - Name and PMKeyS; or
    - Name, User ID and a confirmed email address.
  - If there is not enough information, send a return email requesting the appropriate information before proceeding.
- Reset the member's password.
- Send a return email to the member detailing the CMS User ID and default password.

##### **RETAIN RELEVANT DOCUMENTATION**

The request will be accepted by email only. All emails to be retained by CCSC.

##### **CONTACTS**

##### **CCSC**

Phone: 1800 007 606

Email: corporate.cards@defence.gov.au

#### **4.16 DPC Limit Change**

##### **PURPOSE**

The purpose of this SOP is to outline the standard procedure for changing the credit limit of a DPC

##### **RESPONSIBILITY**

This task is to be undertaken by Corporate Card Support Centre (CCSC)

##### **TIMING**

Within 5 working days

##### **TOOLS**

- NAB Connect
- CAPS

##### **PROCEDURE**

- Limit increases must be on a completed AD773 and signed by both the card holder and Supervisor.
- Limits of \$250,000 or less can be actioned by DPC administrator. Limits of greater than \$250,000 must be referred to the Manager, Corporate Card Support for approval.
- Log onto NAB Connect and process application as per SOP.

##### **RETAIN RELEVANT DOCUMENTATION**

##### **CONTACTS**

Phone: 1800 007 606

Email: corporate.cards@defence.gov.au

##### **NAB**

PCard Support

## **Annex F Defence Informaiton Systems controls**

### **Systems based controls**

1. The following controls were in place prior to the audit:
  - a. The majority of card application requests and amendments were made via web-forms. These forms include *digital signatures*, this enabled Defence to have an audit trail of when the form was submitted / approved by the person;
  - b. Credit cards are only issued to *entitled* personnel. Prior to the audit, the system (CAPS) displayed the employee type and the administrator made the decision to release the application or not to the bank for issuing of the card;
  - c. All new DTC cards were issued with standard approved limits (\$30,000);
  - d. Applicants requiring a different limit requested a change of limit *after* the card had been issued to them;
  - e. Access to *cash* for DPC is by default ***not*** enabled at time of application and was on request for Administrator approval. Applicants requiring cash access requested a cash limit *after* a card had been issued to them;
  - f. Access to cash for DTC is enabled at time of application. Cash limits were controlled at Diners and not established or controlled in Defence Systems;
  - g. Prior to the audit, the Administrator would not allow the approval of an application for an applicant already having an active card of the type applied for. The system would ***displayed/warned*** the administrator;
  - h. Prior to the audit, applicants provided all details on the application. Only Employee Identification and name details were cross referenced to the HR file;
  - i. The primary means of applying for a *limit change* was on the an online form. Limit change applications were justified and signed by the applicant and approved by their supervisor. The GCFO's were not involved in this process;
  - j. Detail changes for the DTC to address, telephone and email addresses were action by:

- (i) By card administrator in CAPS;
  - (ii) By account holder in ProMaster;
  - (iii) By Diners direct contact with cardholder (e.g. when reporting lost/stolen card).
- 2. Changes for Employee name and titled were amended by:
  - a. By card administrator in CAPS;
  - b. By Diners at request of a card administrator.
- 3. The Corporate Cards Centre ran a QA report and identified cardholders that were no longer on the HR file. Members who were not on the file had their credit card cancelled. This reconciliation occurred on a monthly basis. In addition, cardholders no longer requiring their card requested cancellation to corporatecards@defence.gov.au.
- 4. Cardholders who required cash access made a request to Treasury and Banking in the first instance or the administrators.

## **Annex G Defence Informaiton Systems Controls Current**

### **Credit Card systems based improvements post audit**

1. As a result of the audit Defence strengthen controls around the provision of credit cards, active monitoring and fuel card management. Below are the controls that have been strengthened.
2. All applications for credit cards requests and amendments are made via web-forms. These forms include digital signatures. This provides evidence the form was submitted / approved by a particular individual. Where a member or area does not have access to the digital signature a system process has been developed to provide the evidence that the card administrator can process the applicaiton.
3. An additional control that has been implemented is the Auto approval process of applications. A card application will be automatically approved if it passes a series of systems based control tests:
  - a. The application is (digitally) signed;
  - b. The applicant does not already have an active card (of the type applied for);
  - c. The applicant is entitled to a card (of the type applied for);
  - d. The name on the application form matches the Employee ID (HR File lookup – Surname and given name checked);
  - e. The date of birth on the application form matches the HR file date of birth;
  - f. The gender on the application form matches the HR file gender (DTC only);
  - g. A valid address is available on the HR file;
  - h. A valid contact number is available on the HR file;
  - i. A valid CMS user has been provided (required to allocate the card in the Card Management System – CMS);
  - j. A valid default company/cost centre has been provided (required to allocate the card in the Card Management System – CMS).
4. Where an application is not auto-approved it requires the review and release by the card administrator. Certain data can be overridden on the application in the system, an audit trail of manual (and automatic) application reviews is maintained.

5. Credit cards are only issued to entitled personnel. The following table lists Defence employee types and whether personnel in those categories are entitled to a card. The system control checks the rules below and determines if the applicant is entitled to the credit card.

Maintain_Employee_Types_subform		
EmployeeType	DPC Entitled	DTC Entitled
ARMY : RES-LOE	Yes	Yes
RAAF : RES-HSR	Yes	Yes
ARMY : RES-RRF	Yes	Yes
APS	Yes	Yes
APS : EXCHANG	Yes	Yes
ARMY	Yes	Yes
ARMY : CFTS	Yes	Yes
ARMY : FOREIGN	No	No
ARMY : OICDTS	Yes	Yes
ARMY : REG-GAP	Yes	Yes
ARMY : RES-A	Yes	Yes
ARMY : RES-FSL	Yes	Yes
ARMY : RES-I	Yes	Yes
NAVY	Yes	Yes
NAVY : CFTS	Yes	Yes
NAVY : FOREIGN	No	No
NAVY : OICDTS	Yes	No
NAVY : REG-GAP	Yes	Yes
NAVY : RES-A	Yes	Yes
NAVY : RES-I	Yes	Yes
OTHER	Yes	No
PHILANT : ARCS	Yes	Yes
PHILANT : EWS	Yes	Yes
PHILANT : SALARMY	Yes	Yes
RAAF	Yes	Yes
RAAF : CFTS	Yes	Yes
RAAF : FOREIGN	No	No
RAAF : OICDTS	Yes	No
RAAF : REG-GAP	Yes	Yes
RAAF : RES-A	Yes	Yes
RAAF : RES-ES	Yes	Yes
RAAF : RES-HRR	Yes	Yes
RAAF : RES-I	Yes	Yes
APS : N/A	Yes	Yes

Maintain_Employee_Types_subform		
EmployeeType	DPC Entitled	DTC Entitled
ARMY : RES-ES	No	No

6. All new cards are issued with default standard approved limit of \$10,000 for DPC and \$30,000 for DTC. Applicants requiring a different limit can request a change of limit after a card has been issued to them, the Group CFO (SES Band 1 or delegate) is the approver.
7. Credit card limit changes are not auto approved and require the release by a card administrator (in CAPS). Administrators at their discretion can release a request for a limit change under certain circumstances. Such as when a member is stranded on operational duty overseas and has reached the monthly default limit on their card.
8. Access to cash on DPC is by default not enabled at time of application. Applicants requiring cash access may request a cash limit after a card has been issued to them. A business case is submitted to the Group CFO for approval.
9. The system will not allow the approval of an application for an applicant already having an active card of the type applied for. This has been implemented recently in a systems enhancement to CAPS.
10. Applicants provide basic identity data on the application. This is cross referenced to the HR daily data feed, to ensure the provided identify details matched with the identify details in the HR system. Address and contact details are sourced from Corporate Directory data received daily.
11. Amendment to contact details can be amended for DTC;
  - a. By card administrator in CAPS;
  - b. By account holder in ProMaster;
  - c. By Diners direct contact with cardholder (e.g. when reporting lost/stolen card).
12. Defence is currently transitioning to changes only being made on the Defence Corporate Directory (sole source of truth) and automatically sent to Diners. To be completed by Feb 2017.
13. DPC changes are communicated to ANZ. Defence is currently transitioning to changes only being made on the Defence Corporate Directory (sole source of truth) and sent in batch to ANZ. To be completed by Feb 2017

14. A number of additional controls for cancellation of Cards have been implemented. The CAPS system now has the functionality to manage cards not activated. The steps in this process are:
  1. Identify cards not activated within ( $x$ ) days of issue (create batch);
  2. Administrators to email affected cardholders advising them the period they have to activate the card or it will be cancelled;
  3. After the warning period has elapsed administrators initiate the cancellation of cards for the batch. This will cancel (in the next update file to Diners - daily). Only cards which remain un-activated will be cancelled at this time. The administrator has the ability to nominate after how many days the card to be automatically cancelled in the system;
  4. Activation does not apply to ANZ Visa cards (not required).
  5. Card administrators determine the frequency of batches, days un-activated and warning period as required;
  6. Currently performed weekly. Warning email sent at approx 60 days and cancellation after 90 days.
15. All DTC and DPC cards are automatically cross referenced on a daily basis with the HR file. Any active card where the employee is no longer on the HR file or the entitlement to have the card no longer exists will be automatically cancelled.
16. Cardholders no longer requiring their card can request cancellation to [Defence.creditcards@defence.gov.au](mailto:Defence.creditcards@defence.gov.au). Cards are then cancelled in CAPS for DTC or on the ANZ system for DPC. The cancellation request can also come from other sources, all correspondence is loaded into CAPS for audit purposes.
17. If a cardholder requires cash access on their DPC, approval is sought from the Group CFO with a business case and then passed to FASRA approval. FASRA is the Delegate for cash access.



DIRECTORATE OF FINANCIAL ASSURANCE AND COMPLIANCE

# Compliance and Forensic Accounting Framework

---

Work plan for 2016-17

Last updated 12 October 2016

## Document Controls and Approvals

<b>Document Location</b>	Object ID: R27596056
--------------------------	----------------------

<b>Amendment History</b>	<b>Date</b>	<b>Version No</b>	<b>Amendment Details</b>

<b>Distribution</b>	<b>Defence</b>	<b>Position</b>	<b>Date of issue</b>

## Contents

Team Overview .....	4
Staffing.....	4
Executive Summary .....	5
Analysis .....	6
ANAO 2014-15 Closing Audit Report.....	7
a) Finding B3-Estimation of GSI in-year pricing adjustment.....	7
b) Finding C23-Management of Heritage and Cultural Assets .....	8
ANAO 2014-15 Summary of Adjusted and Unadjusted Audit Differences (SAD).....	8
Accounts highlighted in the Defence Annual Report .....	9
Consultants .....	9
Advertising and Market Research .....	11
Legal Expenses.....	12
Accounts where expenditure against the account requires specific delegation. Eg Software .....	13
Accounts with a high inaccuracy coding rate identified in previous years testing .....	14
2016-17 GL Analysis Program.....	16

## Team Overview

There are a number of responsibilities for this team: Forensic analysis and Compliance and the Gifts and Hospitality register. These functions are mainly responsible for ensuring compliance with the *Public Governance and Performance Accountability Act 2013* and testing to provide assurance to the Minister that our data within the financial statements are accurate.

The outcome of this work is a key priority for the team, regardless of the task – there must be a genuine purpose and use for performing the work, the outcomes achieved must be assessed against goals, and continuous improvement and feedback must become routine.

Forensic analysis is the analysis of financial data contained within the Financial information systems, which focuses on:

- Miscoding and or Vendor
- Misuse of Commonwealth funds; and
- Fraud.

This function forms part of DFAC's core business and is performed to enhance the financial controls framework and controls testing. This strategy has been engaged to assist with Defence complying with the Australian Accounting Standards AASB101 which requires Defence to present fairly the department's financial position, performance and cash flows. In this respect DFAC will be reviewing expense transactions across the general ledger (GL) account codes. DFAC's focus with this body of work will be on GL accounts and merchant categories.

This body of work is performed not only to provide assurances that Defence is complying with relevant Accounting Standards, but it is also performed to shape and alter behaviours. This work also ensures effective and appropriate policy and legislation are complied with and also allows for forecasting future trends and identifying emerging areas of concern or weakness ensuring that we are value-adding to outcomes intended from this work.

## Staffing

The team currently consists of six staff, one part time, with a linear reporting structure. The scope of work to be performed within the overall area of responsibility will be determined based on order of priority set by management and the availability of resources.

Responsibilities within the team will be allocated with consideration given to: promoting learning and development opportunities, providing work of interest at a suitable level, and allowing ownership of specific tasks.

Name	Level	Availability	Primary responsibility
<b>Michael Sharp</b>	EL1	Fulltime	Manage the forensic accounting process Manage the Compliance process undertaken by the team. Manage the Gifts and Hospital process.
<b>Jenna Black</b>	APS 6	Part-time 4 days	Forensic analysis, Monthly reporting
<b>Paul Tarrant</b>	APS 6	Fulltime	Forensic GL Analysis and GHS responsibilities
<b>Ivana Cikara</b>	APS 6	Fulltime	Forensic GL Analysis- compliance consolidation
<b>Thi Tran</b>	APS 5	Fulltime	Forensic GL Accounting
<b>Heather Rogers</b>	APS 5	Fulltime	Forensic GI Accounting and Objective manager

## Executive Summary

The *Public Governance and Performance Accountability Act 2013* (PGPA Act) underpins the financial framework in respect to the use of money and resources within the Australian Government and is an important feature of an accountable and transparent public sector.

Essentially the PGPA Act requires the Commonwealth:

- To meet high standards of governance, performance and accountability; and
- To provide meaningful information to Parliament and the public; and to sue and manage public resources properly; in addition to working cooperatively with others to achieve common objectives.

In meeting this function the Directorate of Financial Assurance and Compliance (DFAC) is designated within the Chief Finance Officers Group (CFOG) to report on financial assurance activities that have been undertaken during a set period. Therefore to meet this mandate DFAC's 2016-17 GL Analysis program, will concentrate on the analysis of the financial data contained within Defence financial information systems focusing on miscoding of GL transactions.

In order to comply with the Australian Accounting Standards AASB 101, Defence Financial Reports must present fairly the financial position, financial performance and cash flows of an entity. The Department of Finance has also published a Resource Management Guide 135 (RMG 135) which provides guidance on Annual Report requirements. These two documents form the basis of DFAC's GL Analysis program.

In developing the 2016-2017 GL Analysis Program, the following sources were considered:

1. The Australian National Audit Office (ANAO)
  - 1.1 Audit Strategy,
  - 1.2 Audit Findings,
  - 1.3 Summary of Adjusted and Unadjusted Audit Differences.
2. Accounts highlighted in the Defence Annual Report e.g. Consultants.
3. Accounts with high inaccurate coding rates identified in the 2015-16 testing program; and
4. Accounts where expenditure against the account requires specific delegation. e.g. Software..

## Analysis

### 2.1 ANAO

#### 2.1.1 ANAO 2014-15 Audit Strategy

The ANAO's 2015-16 Audit Strategy for Defence identified two risk areas:

- a) Executive Remuneration; and
- b) Grant and Support Payments.

#### a) Executive Remuneration

Executive remuneration within Defence is paid in various forms such as salaries, superannuation leave, leased motor vehicles, car parking, housing; and or medical benefits to name a few.

Account Number	Account Name	Definition	Includes	Excludes
21016	Leased vehicle non SES operating costs	Operating costs for non-SES leased vehicles.	Fuel, cleaning, car wash, repairs, service, etc.	Lease agreement payments.
24931	Op lease EVS SES vehicle	Fixed lease amounts for Operating Lease Contracts (Lease Agreements) for the Executive Vehicle Scheme (EVS) vehicles only.	EVS Lease payments (includes interim vehicles under EVS) for SES officers. Stamp Duty if applicable. Ensure that Vehicle Rego number is quoted in the ROMAN payment document text field.	Pass on Costs' such as fuel, non-contracted maintenance services and fees use 21046. Costs for pool and/or staff plated vehicles use 24932. Amounts for CPI and market rates in Operating Lease payments use 24960. Hire expenses use 21022.
21046	Leased vehicle SES operating costs	Only use for the Executive Vehicle Scheme (EVS) vehicles. Operating costs for EVS leased vehicles for SES officers.	Fuel, cleaning, car wash, repairs, service, mobile phone hands free kit and installation, etc for all EVS SES officers, Ensure that Vehicle Rego number is quoted in the ROMAN payment document text field.	Lease agreement payments for EVS refer 24931. All Non EVS vehicles.
24933	Op lease non SES overseas vehicle	Fixed lease amounts for Operating Lease Contracts (Lease Agreements) for vehicles for non-SES staff overseas posts.		Amounts for CPI and market rates in Operating Lease payments use 24960. Other operating costs associated with the lease (fuel, cleaning, repairs, services) use 21016. Hire expenses use 21022.

## b) Grants and Support Payments

Defence contributes and supports a number of other government entities, private sector organisations and individuals through the provision of grants which should be identified as a grant in the financial systems and recognised as an expense when incurred. This requirement will be extremely important when compulsory annual reporting requirements under the *Superannuation Laws Amendment (2015 Measures No 5) Act 2015* come into effective 1 July 2017.

Account Number	Account Name	Definition	Includes	Excludes
12019	s.31 Sponsorship, grants, subsidies for Dept activ	Sponsorships, grants, subsidies & contributions received to fund departmental activities .Sponsorship is an arrangement where sponsor provides money or in kind support for an activity in return for specified benefits Refer DI(G) Pers 25-7 Annex D.	Air Show and sporting clubs sponsorship. Sponsorship of a Defence-run conference by the public or private sector.	Grants from FMA Act Agencies.
25234	Grants to not for profit entities	Grants provided to 'not for profit' private sector entities including individuals.	Grants to individuals for Military History Research. Grants to research institutions ie RUSI.	Grants to public sector or 'for profit' entities.
25235	Grants to private sector	Grants to 'for profit' private sector entities.	All DMO grant payments made to Defence industry sector. Sponsorship categorised as a grant. See DI(G) PERS 25-7 Annex I.	Grants to public sector or 'not for profit' entities.
25237	Grants to state & territory governments	Grants provided to state and territory governments.	Grants provided to state and territory governments. Sponsorship categorised as a grant. See DI(G) PERS 25-7 Annex I.	A payment to a State to Territory that is made for the purposes of the Federal Financial Relations Act 2009.
25239	Grants overseas	Grants to overseas entities.	Grants to overseas entities including NGOs. Sponsorship categorised as a grant. See DI(G) PERS 25-7 Annex I.	
25240	Grants to related entities	Grants to related Commonwealth Government entities defined as related by the FMO's and other guidance (including Defence/DMO).	Grants to AAFCANS, ASPI and any other CAC Act bodies. Sponsorship categorised as a grant. See DI(G) PERS 25-7 Annex I.	Grants to FMA Act Agencies.

## ANAO 2014-15 Closing Audit Report

The 2014-15 ANAO Closing Audit Report identified findings that have linkages to the GL analysis program. The following two findings are:

- Finding B3-Estimation of General Stores Inventory (GSI) in-year pricing adjustment.
- Finding C23-Management of Heritage and Cultural Assets.

### a) Finding B3-Estimation of GSI in-year pricing adjustment

During sample testing the ANAO identified a number of assets that:

- were erroneously capitalised into General Stores Inventory including prepayments for licences or ongoing IT support including components in the base price of inventory such as supplier mark-ups; and
- represented administrative overheads that do not contribute to bringing inventories to their present location or condition in accordance with AASB102 paragraphs 16©<sup>1</sup>.

<sup>1</sup> Examples of costs excluded from the cost of inventories and recognised as expenses in the period in which they are incurred are:  
(a) abnormal amounts of wasted materials, labour or other production costs; (b) storage costs, unless those costs are necessary in the production process before a further production stage; © administrative overheads that do not contribute to bringing inventories to their present location and condition; and (d) selling costs.

The following GSI balance sheet accounts can be examined for evidence of transactions that should **not** be recorded as GSI.

Account Number	Account Name	Definition
53021	Inventory - GSI (n/curr)	The value of GSI inventory holdings at period end, that belong to Defence and are expected to be consumed beyond the next year.
53041	Inventory contractor held - GSI (Curr)	The value of GSI inventory holdings that belong to Defence, but are held by third party contractors and which are expected to be consumed within the next year.
53042	Inventory contractor held - GSI (N/Curr)	The value of GSI inventory holdings that belong to Defence, but are held by third party contractors and which are expected to be consumed later than 12 months from now.
53020	Inventory - GSI (curr)	The value of GSI inventory holdings at period end, that belong to Defence and are expected to be consumed within the next year.

## b) Finding C23-Management of Heritage and Cultural Assets

The ANAO found during this process that not all assets recorded in the heritage and cultural asset class met the criteria as per the accounting standards and the Financial Reporting Rules (note nil inclusions/exclusions).

Account Number	Account Name	Definition
12077	Assets now recognised - Heritage and cultural	This account is an offset account for the balance sheet recognition of assets that have been expensed in a prior financial year. This account relates to Heritage and Cultural Assets recognition.
52904	Gross book value-Heritage and cultural-ROMAN	This account is used for Heritage and Cultural Assets that are on the ROMAN Asset register. This is a control account.
52906	Gross book value-Heritage and cultural	This account is used for Heritage and Cultural Assets that are NOT on the ROMAN Asset register. This is not a control account.
52933	Assets held for sale - Heritage & cultural	Assets that are NOT on the ROMAN Asset Register and are planned to be sold should be transferred to this account.
54104	Assets held for sale - Heritage and cultural	Heritage and cultural assets available for immediate sale and planned to be sold within the next 12 months.

## ANAO 2014-15 Summary of Adjusted and Unadjusted Audit Differences (SAD)

Transaction and accounting errors identified by the ANAO are reported in the ANAO Summary of Adjusted and Unadjusted Audit Differences. The GL accounts impacting on two audit differences below should be considered for future GL Analysis.

Description	Line item	Statement of Financial Position		Statement of Comprehensive Income	
		DR	CR	DR	CR
To capitalise powerboards which were over the capitalisation threshold	Other plant and equipment(Ac 5204)	159,621.00			
	ICT User Hardware Purchase and Support (Ac 21428)				159,621.00
To correct IT hardware incorrectly expensed	DMO Sustainment Contract Expense (AC2800)				3,866,803.00
	Gross Book Value SME (Ac 52306)	3,866,803.00			



## Accounts highlighted in the Defence Annual Report

The following three expense items are separately reported in the Defence Annual Report, they are:

- a) Consultants
- b) Advertising and Market Research; and
- c) Legal Expenses

### Consultants

The *Public Governance Performance and Accountability Act 2013 (PGPA)* Resource Management Rule 17AA, prescribes the requirements for annual reports for non-corporate Commonwealth entities. The annual report must include the following for consultants, with points **2** and **4** having particular relevance to the GL Analysis program. These requirements are:

- (1) the number of new contracts engaging consultants that were entered into during the period
- (2) the total actual expenditure during the period on all such contracts (inclusive of GST);**
- (3) the number of ongoing contracts engaging consultants that were entered into during a previous reporting period; and
- (4) the total actual expenditure during the period on those ongoing contracts (inclusive of GST).**

Accounts with consultant references are listed below.

Account Number	Account Name	Definition	Includes	Excludes
21026	Develop capability definition documents	Expense associated with development of Capability Definition documents. (When the expense relates to contract for the engagement of an external additional resource to work for Defence, a ROMAN External Service Provider (ESP) FIELD must be used.)	(Refer CFO Glossary for ESP definitions (Consultant, PSP & Contractor).)	
21711	Recruitment services	Expenses associated with the recruitment of new employees not required to be reported elsewhere in the Chart of Accounts.	(When expense relates to contract for engagement of external additional resource to work for Defence, ROMAN External Service Provider FIELD must be used - refer CFO Glossary for ESP definitions (Consultant, PSP&Contractor).) Recruitment fees, scribes.	ADF Recruitment advertising use 21750, APS Recruitment advertising use 21761. Travel associated with recruitment and enlistment use 21315.

Account Number	Account Name	Definition	Includes	Excludes
22000	Repair and overhaul - OP&E	Repair&overhaul expenses of other plant&equipment(OP&E).(When the expense relates to contract for engagement of external additional resource to work for Defence, ROMAN ESP FIELD must be used-CFO Glossary for definitions(Consultant, PSP & Contractor).)	Outsourced repair&overhaul contracts for OP&E.Contracts primarily for repair&overhaul where technical/engineering services are embedded in the contract.Materials/labour for repair&overhaul of OP&E.	Repair and maintenance of buildings and SME. Contracting of ESPs specifically for technical/engineering services use 22042.
22042	Technical services	Expense primarily associated with provision of Technical/Engineering Services.(When the expense relates to contract for engagement of an external additional resource to work for Defence, a ROMAN External Service Provider (ESP) FIELD must be used.)	(Refer CFO Glossary for ESP definitions (Consultant, PSP & Contractor).) Contracts primarily for technical/engineering services.	Travel use 21319. Costs (other than the contract payments) are to be posted to the appropriate expense account.
25204	Accounting & Financial Support	Expense associated with provision of Financial & Accounting related services & advice (when the expense relates to contract for engagement of external additional resource to work for Defence, ROMAN External Service Provider (ESP) FIELD must be used).	Refer CFO Glossary for ESP definitions (Consultants, PSP & Contractor).	
22035	Technical services - Ships	Used by CASG-MSD for expenses of an engineering nature against major platforms.(When the expense relates to contract for the engagement of an external additional resource to work for Defence, ROMAN External Service Provider(ESP) FIELD must be used.)	(Refer CFO Glossary for ESP definitions (Consultant, PSP & Contractor).)	
21418	ICT administration charges in bundled contracts	Expenses relating to the administration component built into a bundled ICT contract.	Administration payments made to an External Service Provider (ESP) as part of a bundled ICT contract.	The purchase, maintenance and support of ICT hardware and software and expenses associated with satellite usage (use GL 21402), spectrum (use GL 21415) and carriage such as phone calls and internet usage (use GL 21400).
21440	Software services	Expenses relating to the configuration, customisation, upgrade, sustainment and support of systems and application software.	Includes External Service Provider (ESP) and other expenses related to the configuration, customisation, upgrade and support of software.	For software licence fees (use GL 21416). Also excludes the purchase, maintenance and support of ICT hardware and expenses associated with satellite usage (use GL 21402), spectrum (use GL 21415) and carriage such as phone calls and internet usage (use GL

## Advertising and Market Research

Advertising and Market Research amounts are to be report in the Defence Annual Report when they are paid by, or on behalf of Defence. A list of the relevant GL's that will be targeted during this period are listed below.

Account Number	Account Name	Definition	Includes	Excludes
21711	Recruitment services	Expenses associated with the recruitment of new employees not required to be reported elsewhere in the Chart of Accounts.	(When expense relates to contract for engagement of external additional resource to work for Defence, ROMAN External Service Provider FIELD must be used - refer CFO Glossary for ESP definitions (Consultant, PSP& Contractor).) Recruitment fees, scribes.	ADF Recruitment advertising use 21750, APS Recruitment advertising use 21761. Travel associated with recruitment and enlistment use 21315.
21750	Advertising costs - ADF recruiting	Australian Defence Force recruitment advertising only. In Purchase Order/Invoice - text field must include media type(TV/paper/direct mail etc).	ADF recruitment. Account data used to compile schedule of advertising cost (TV/newspaper etc) for annual report.	All other forms of recruitment, eg APS Recruitment advertising use 21761. Hire of premises/facilities used during recruitment. Purchase of signs, banners, pamphlets and other printing items.
21761	Advertising Costs - Non ADF Recruiting	All advertising expenses not specifically mentioned elsewhere in the chart. In Purchase Order/Invoice text field - must include type of advert (civilian recruit/public notices/event advert/tender) & media type (TV/paper/direct mail etc).	APS recruitment. Account data used to compile schedule of advertising cost (TV/newspaper etc) for annual report.	ADF Recruitment advertising use 21750. Hire of premises/facilities used during recruitment. Purchase of signs, banners, pamphlets and other printing items. Provision of sponsorship use 21762.
21762	Provision of sponsorship	Any sponsorship arrangements provided.	Sponsorship advertising	APS recruitment advertising use 21761 ADF Recruitment advertising use 21750. Hire of premises/facilities used during recruitment. Purchase of signs, banners, pamphlets and other printing items.

## Legal Expenses

Legal expenses are reported separately in the Defence Annual Report, with the relevant GL's to be targeted for the 2016-2017 GL Analysis program listed below.

Account Number	Account Name	Definition	Includes	Excludes
20773	Travel ADF - Legal/discipline	Conditions of service provide for Defence funding for legal or disciplinary action.	Travel as an escort officer. Travel related to the defence of military members and witnesses. Travel of Military Judges and Military Jury members. Accompanied excess baggage-airfare related.	Travel Management Company Fees and Travel WoAG Fees use 21309
21712	DFDA Legal expenses/disbursements	Expenses incurred in relation to DFDA matters.	Witness reimbursements. Transcription Services. Other costs associated with the conduct of DFDA Summary procedures and Australian Military Court (AMC) Trials.	Travel in relation to DFDA Summary procedures and AMC trials.
21722	Legal professional fees	Professional fees Defence legal panel.	Professional fees tied to the Australian Government Solicitor (AGS) (legal).	Probity Advisory Services use 21035.
21730	Legal assistance at Commonwealth expense	Legal expenses authorised in accordance with F8-2 of Financial Delegation Manual (FINMAN 2).		
21713	Reserve legal officers fees	Reserve legal officers' fees.		
21715	Legal disbursements	Commonwealth disbursements (legal).		

## Accounts where expenditure against the account requires specific delegation. Eg Software

FINMAN 2 – Part 3: Software Purchases Part 4: *ICT Hardware Purchases* contains *Specific* delegations for ICT purchases of Software and Hardware. Previous reviews have identified instances where these delegations have not been applied correctly; therefore DFAC will also target these transactions in the GL Analysis program. A list of the relevant GL's can be found below.

Account Number	Account Name	Definition	Includes	Excludes
52700	Gross book value - Software pur	This account is used for Software purchased that are NOT on the ROMAN Asset register. This is not a control account.	Nil	Nil
52704	Gross book value - Software pur- ROMAN	This account is used for Software purchased that are on the ROMAN Asset register. This is a control account.	Nil	Nil
52962	Restoration provision - Software purchased	This account should contain the amount of money that it is expected to cost to restore the asset to saleable condition. This account should only be used with written approval from the Group Asset Management Team.	This account recognises the asset for restoration provision for asset class - Infrastructure (i.e. all entries DR 52962 and CR 30166).	Nil
21418	ICT administration charges in bundled contracts	Expenses relating to the administration component built into a bundled ICT contract.	Administration payments made to an External Service Provider (ESP) as part of a bundled ICT contract.	The purchase, maintenance and support of ICT hardware and software and expenses associated with satellite usage (use GL 21402), spectrum (use GL 21415) and carriage such as phone calls and internet usage (use GL 21400).
21425	ICT network hardware - purchase and support	Expenses relating to the physical ICT infrastructure used to move information/data to, from and within the DIE (Defence Information Environment).	Expenses for the purchase, maintenance and support of network hardware such as cabling, switches, routers, PABXs and patch leads associated with the Wide Area or Local Area Networks (WAN or LAN).	Any of the included items above the \$2,000 capitalisation threshold (use GL 23212 for cost centres or GL 23006 for projects with a real WBS). Also excludes hardware associated with servers and server rooms (use GL 21450) and Defence user hardware
21428	ICT user hardware - purchase and support	Expenses relating to the physical ICT hardware and peripherals that are used by the Defence end user to access applications and data.	Expenses for the purchase, maintenance and support of user hardware such as keyboards, mice, desktops, laptops, computer monitors, iPads, personal storage devices (e.g. USBs), printers, MFDs, printer cartridges, faxes, scanners, burners etc.	Any of the included items above the \$2,000 capitalisation threshold (use GL 23212 for cost centres or GL 23006 for projects with a real WBS). Also excludes network hardware such as cabling, switches, routers and patch leads (use GL 21425) and hardware as
21440	Software services	Expenses relating to the configuration, customisation, upgrade, sustainment and support of systems and application software.	Provider (ESP) and other expenses related to the configuration, customisation, upgrade and support of software.	For software licence fees (use GL 21416). Also excludes the purchase, maintenance and support of ICT hardware and expenses associated with satellite usage (use GL 21402), spectrum (use GL 21415) and carriage such as phone calls and internet usage (use GL
21450	ICT systems hardware - purchase and support	Expenses relating to physical hardware associated with servers and server rooms.	The purchase, maintenance and support of mainframe, midrange, storage, file and print servers. Also includes hardware associated with server rooms such as racks, Uninterruptible Power Supply (UPS) devices and devices to monitor the humidity temperature	Any of the included items above the \$2,000 capitalisation threshold (use GL 23212 for cost centres or GL 23006 for projects with a real WBS). Also excludes network hardware such as cabling, switches, routers and patch leads (use GL 21425) and Defence end

## Accounts with a high inaccuracy coding rate identified in previous years testing

The following accounts during the 2015-2016 GL Analysis Program were identified as areas of concern due to a high error rate and will be accounts also targeted during this period. The accounts are:

### **21151 Employee family support**

Items in this GL are miscoded, or not relevant to the actual definition. Some of the incorrect coding (as per the description and documentation provided by Groups) include vehicle cleaning, cleaning; defence diaries; toll account; craft supplies for kids; snacks for kids; graduation cake supplies; back order notepads; storage tubs for office use and catering.

### **21022 Hire and other fees**

Items transacted to this GL are reimbursements for participating in ADF sports (e.g. Cairns Ironman triathlon, Port Macquarie Ultraman, ADFSC Triathlon); reimbursement of fuels for hire car; pillow feathers; food for ice skating, medical equipment, car hire; deck stores (inc soaps, garbage bags and cleaning products); and transportation.

### **21941 ADF training - Non military**

Items transacted to this GL include RACGP memberships; software; storage cases; medical equipment, private rock climbing tuition; shipping and handling; medical indemnity cover; IMIMS Annual subscription; travel and accommodation.

### **21171 Contract labour**

Items transacted to this GL include temp recruitment; cocktail dinner, Melbourne cup function, and lock repairs.

### **21416 Software**

Software delegations appear to be incorrect on a large number of transactions (i.e. not signed off by CIOG or equivalent Delegates), and there appear to be software purchased by Groups where CIOG has Enterprise Agreements with certain vendors (e.g. Microsoft, Oracle, Adobe etc) and Groups have purchased software outside the arrangement.

This conclusion has been drawn from viewing the documentation provided by the Finance Data Centre and also credit card transactions that have been provided by Groups.

### **23214 Accountable and consumables - OP&E**

Some of the items in 23214 (from the text description and documentation sighted) include, petrol; venue hire; car seat covers; replacement keys, printer cartridges, plaques; reimbursement of golf tees; sheets; table clothes; can of tennis balls; WHS assessment; Xmas tree and paper; rations and guitar strings. The error in this GL comes from the incorrect coding of the Purchase Order (PO)

### **23212 Accountable and consumables - ICT hardware**

The miscoding for this GL comes from the PO and viewing quotes supplied by the company. Items clearly miscoded are stationery and postage, with some items actually being classed as assets. .

### **23213 Accountable and consumables - Software**

This GL consists of software licences and renewals under the threshold that should be ideally coded to 21416.. There are also items that are not software related which include wall chargers, USB

cables, and printer cartridges. There are also items that are over the 23213 threshold and should be coded to the software asset account - e.g. PO 4500961963.

## 2016-17 GL Analysis Program

An examination of GL Accounts over a four month period with a dollar value exceeding **\$250.00** will be sufficient to draw a conclusion of the accuracy of coding within the targeted accounts.

Therefore each staff member involved in the GL review process will be allocated a list of accounts to examine, with the current arrangements for recording testing results enhanced by:

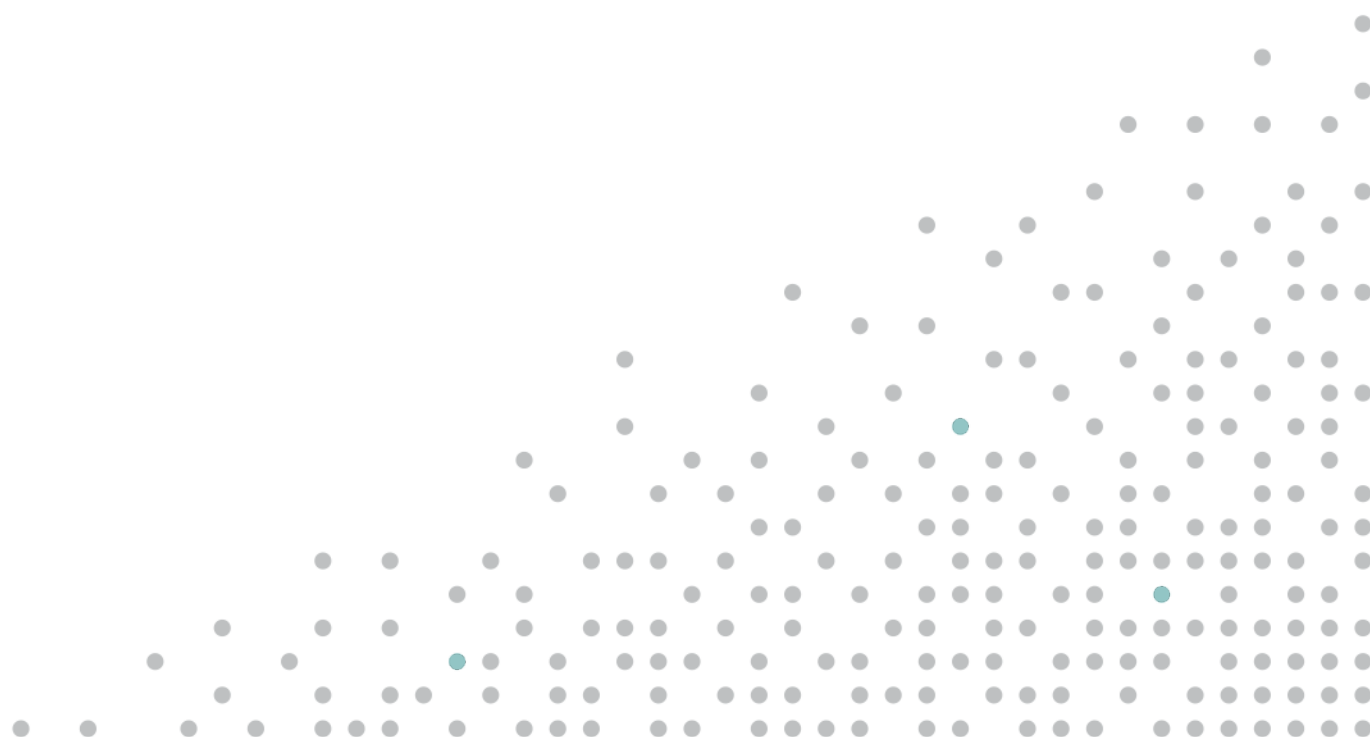
- a) Having one register for all transactions sampled.
- b) Having a standardised template emailed by DFAC GL processors asking for documentation.
- c) Identifying instances of non-compliance against the PGPA Act and advising Groups where instances have not been recorded in the Compliance Reporting Register in SharePoint.
- d) Placing unrecorded instances of potential breaches against the PGPA Act in the Group external parties folder in Objective, giving Groups an opportunity to view non-compliances that has been identified and discuss as required; and
- e) Providing transactions that have been identified as miscoded, into the external parties folder in Objective so Groups are aware of the miscoding identified and Groups can then process the appropriate journals, or have an opportunity to review and comment on the analysis provided by DFAC.

## Annex A – Draft DFAC GL Analysis Work Plan





**Australian Government**  
**Department of Finance**



# **Facilitating Supplier Payment Through Payment Card**

## **Resource Management Guide No. 416**

NOVEMBER 2016

© Commonwealth of Australia 2016

ISBN: 978-1-922096-61 (Online)

With the exception of the Commonwealth Coat of Arms and where otherwise noted, all material presented in this document is provided under a Creative Commons Attribution 3.0 Australia (<http://creativecommons.org/licenses/by/3.0/au>) licence.



The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the CC BY 3 AU licence.

### **Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are detailed on the following website:  
[www.dpmc.gov.au/government/its-honour](http://www.dpmc.gov.au/government/its-honour).

### **Contact us**

Please direct questions or comments about the guide to:

Department of Finance  
Procurement Policy Branch  
1 Canberra Avenue  
Forrest ACT 2603

Email: [procurementagencyadvice@finance.gov.au](mailto:procurementagencyadvice@finance.gov.au)

Internet: [www.finance.gov.au/procurement](http://www.finance.gov.au/procurement)

# Contents

<b>Facilitating Supplier Payment Through Payment Card</b>	<b>1</b>
Audience	4
Key points	4
Resources	4
<b>Part 1 – Policy</b>	<b>5</b>
<b>Part 2 – Guidance</b>	<b>5</b>
<b>Part 3 – Definitions</b>	<b>6</b>
Figure 1: Decision tree on making supplier payments via a payment card	7

## Audience

This Guide is relevant to all non-corporate Commonwealth entities (NCEs). It is particularly relevant to Chief Financial Officers (CFOs) and their staff, and officials who are responsible for the NCEs internal controls and processes.

## Key points

This Guide:

- outlines the Government's policy on payment cards as the preferred method to pay suppliers for eligible payments valued below \$10,000; and
- uses terms as defined in the Commonwealth Procurement Rules.

## Resources

This guide is available on the Department of Finance website at [www.finance.gov.au](http://www.finance.gov.au).

Other relevant publications include:

- [\*Commonwealth Procurement Rules\*](#).
- Additional information on this policy: <https://www.finance.gov.au/resource-management/spending/credit-card-policy/additional-information/>.

## Part 1 – Policy

1. NCEs must establish processes that promote payment cards as a preferred option for eligible payments to suppliers valued below \$10,000.
2. NCEs must, to the extent practicable, provide suppliers an opportunity to request payment via a payment card for amounts below \$10,000.
3. NCEs must make payment via a payment card where requested by a supplier for eligible payments. Where practicable, payment should be made at the point of sale. A tax invoice (receipt) must be provided by the supplier for the payment.
4. The policy does not require payment by NCEs on disputed amounts. Where an amount is disputed, the NCE may request to make payment after receiving an invoice.

## Part 2 – Guidance

5. The policy facilitates timely payment to suppliers, assists with their cash flow, and reduces the cost to business in supplying to the Commonwealth.
6. The policy requires NCEs to maintain policies to facilitate the timely payment of suppliers through payment card processes. NCEs may choose to extend this policy to non-eligible payments or payments above \$10,000 in line with their business needs.
7. NCEs are to use payment card processes at the point of sale for amounts below \$10,000, in preference to suppliers issuing invoices.
8. Suppliers may be unaware of the preferred payment option and reasonable efforts should be made to make them aware of the opportunity. This should occur prior to receiving goods or services.
9. NCEs must pay via a payment card where the:
  - payment is an eligible payment and valued under \$10,000 (inclusive of GST and merchant service fees<sup>1</sup>);
  - supplier can accept and request payment via a payment card; and
  - merchant service fees charged to the NCE are reasonable for the type of card being used and are sufficiently disclosed prior to payment being made.
10. NCEs should consider paying suppliers via a payment card, but may reasonably seek to pay via an invoicing arrangement when:
  - amounts owed are at, or above, \$10,000;
  - paying incremental or milestone payments, irrespective of whether the collective value of the payments is below \$10,000;
  - the supplier requests payment via an invoicing arrangement;
  - the supplier seeks payment through non-widely recognised payment cards;

---

<sup>1</sup> Costs due to the supplier (merchant service fees) may be passed on to the NCE when facilitating payment via a payment card. Merchant service fees are required to be limited to 'reasonable cost' for accepting the payment which may vary on the card scheme used. Further guidance on merchant service fees is available from the Reserve Bank of Australia in *Guidance Note: Interpretation of the Surcharging Standards* ([www.rba.gov.au](http://www.rba.gov.au)).

- paying other Commonwealth entities;
- paying overseas-based suppliers; or
- paying third-parties on behalf of the NCE.

11. NCEs are responsible for ensuring that relevant internal guidance is maintained to give effect to the policy.

## Part 3 – Definitions

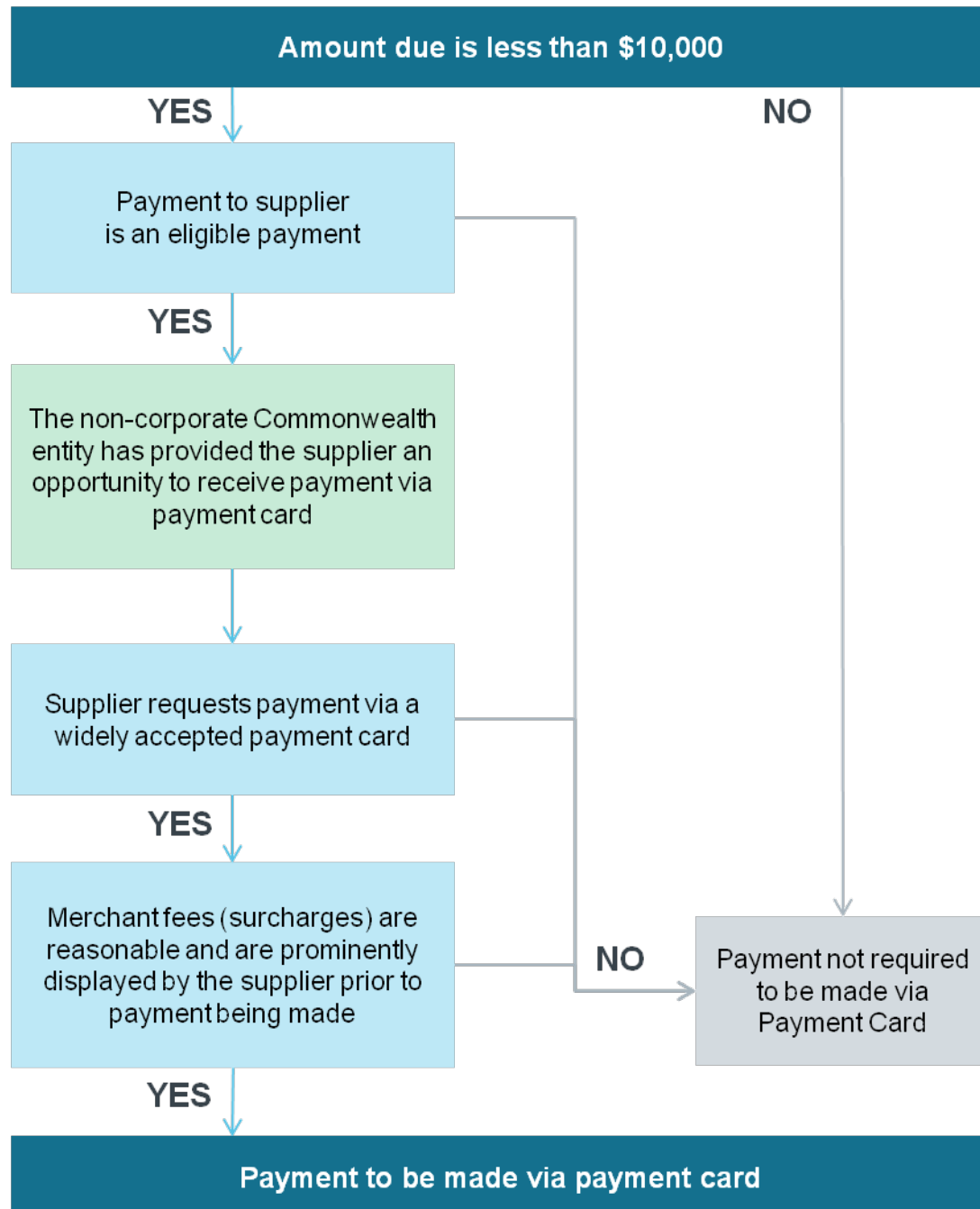
**Business Day** means a day that is not a Saturday, Sunday, public holiday or bank holiday in the place where the act is to be performed.

**Disputed Amount** means any amount issued by a supplier that in the NCE's opinion, is incorrectly calculated and/or not due for payment.

**Eligible Payment** means a payment with a value less than \$10,000 (inclusive of GST and merchant service fees) due to a supplier that is not associated with a multiple-payment contract, or standing offer arrangement. Eligible payments may include payments made as a result of purchase orders. Eligible payments do not include payments due where the NCE has automated invoice payment processes that pay suppliers within five business days of receiving a correctly rendered invoice.

**Payment Card** means credit, debit cards, charge cards or any other type of Commonwealth issued card, including virtual cards that are authorised to pay suppliers for goods or services received at the point of sale. Examples of widely recognised payment cards include American Express, Diners Club, MasterCard and Visa.

**Figure 1: Decision tree on making supplier payments via a payment card**



**Department of Defence**  
**Credit Card Governance**  
**January 2016**

Credit Cards are an important and commercially sensible method of transferring funds to Defence's Vendors.

Credit Cards sit within a matrix of payment mechanisms, some of which are available to line managers and some are only available to the Treasury and Banking Branch within the CFOG. The full suite of payment mechanisms and their relevance are contained in **Attachment 1**.

It is Government policy that all payments to vendors less than \$10,000 should be by Credit Card unless a vendor does not accept a Credit Card. (Department of Finance Resource Management Guide No. 416 Facilitating Supplier Payment through Payment Card)

Each payment mechanism has their particular inherent risks, efficiencies, effectiveness and cost profiles. The use of a particular mechanism is therefore considered in light of their profile. A summary of factors to be considered using a Credit Card are listed in **Attachment 2**.

The key governance elements of Credit Card management are as follows:

1. Travel Card spending limits are set at \$10,000 on a default basis. Business cases for increased limits are to be provided to Group CFO's (or their delegate) for approval. Credit Card limits may be reduced depending on usage patterns.
2. Purchase Card spending limits are set at \$30,000 on a default basis. Business cases for increased limits are to be provided to Group CFO's (or their delegate) for approval. Purchase Card limits may be reduced depending on usage patterns.
3. Virtual Card spending limits are set at \$500,000 on a default basis. Business cases for increased limits are to be provided to Group CFO's (or their delegate) for approval. Virtual Card limits may be reduced depending on usage patterns. Virtual Travel Cards are to be used only when transaction volumes demand or as determined by the Group CFO.
4. The Group CFO's (or their delegate) will annually (first quarter of each financial year) review the following to determine whether to retain or alter:
  - Individual Credit Card spending limits
  - Individual Credit Card cash transferral limits
  - Virtual Credit Card limits
  - Merchant Categories
  - Unused Credit Cards



5. Purchasing card cash transfer limits are set of \$0 on a default basis and business cases for increased limits are to be provided to Group CFO's for approval.
6. Credit Card transactions will be monitored monthly with particular focus on the merchant categories listed at **Attachment 3**.
7. Merchant categories barred from use and that have been disabled are at **Attachment 4**.
8. All Credit Cards that are not activated within 90 days will be cancelled. Reapplication can be made through the usual process.
9. All physical Credit Cards are to be subjected to unique pin codes. Non Aviation Fuel Cards are to be reset from the default pin on issue to either a unique pin code or a unit specific code within 7 days of issue.
10. These arrangements will be written into relevant policy document, and are effective from 18/01/2016.
11. Any Credit Card transactions which are not supported by adequate explanation will be referred to the audit and investigation branch.

**Attachment 1**

<b>Payment Method</b>	<b>System Used</b>	<b>Valid Currencies</b>
Direct Entry (EFT)	ROMAN	Local & Foreign Currencies
Cheque	ROMAN	Local & Foreign Currencies
Manual Direct Entry	RBANet - Treasury & Banking use only	Local & Foreign Currencies
Manual (Collect) Cheque	Treasury & Banking use only	Local & Foreign Currencies
Credit Card - Credit Payment	Credit Card	Local & Foreign Currencies
Credit Card - EFT Payment	Credit Card	Local & Foreign Currencies
Credit Card - Cash Withdrawal	Credit Card	Local & Foreign Currencies
Urgent/Immediate Manual Direct Entry	Treasury & Banking use only	AUD only

## Attachment 2

### Credit Card Vs System Payments

#### Relatively Worse

#### Relatively Better

System	Corporate Information	CC
CC	Cost	System (CC)
CC	Procurement Adherence	System (CC)
CC	Authorised Use	System (CC)
CC	Personal Risk	System (CC)
System	Vendor Settlement Speed	CC
System	Manager Convenience	CC
System	Settlement Terms	CC
System	Average Speed of Transactions	CC

**Attachment 3**

**DEFENCE CREDIT CARDS**

<b>CATEGORIES TO BE MONITORED (54)</b>	
<b>Merchant Number</b>	<b>Description</b>
1600	Real Estate Agent
1830	Traffic and Parking Fines
2110	Theatres & Ticket Services
3050	Liquid/Wines & Spirits
3200	Jewellery/Watches/Clocks
3320	Furs
3500	Duty Free
3835	Duty Free
3844	Messenger Services
3856	Inflight Sales
3882	Cheque Cashing
4400	Messenger Services
4722	Travel Agencies and Tour Operations
4723	Package Tour Operations ( Germany Only)
5094	Precious stones, metals, watches & jewellery
5193	Florist Supplies, Nursery Stock and Flowers
5271	Mobile Homes Dealers
5300	Wholesale Clubs
5309	Duty Free Shops
5592	Motor Home Dealers
5598	Snowmobile Dealers
5600	Inflight sales
5681	Furries and Fur Shops
5931	Used Merchandise and Second-hand Stores
5932	Antique Stores
5933	Pawn Shops
5937	Antique Reproductions
5944	Clock, Jewellery, Watch and Silverware Store
5948	Leather Goods and Luggage Stores
5960	Direct marketing insurance services
5962	Direct marketing -Travel Related Arrangement Services
5963	Door to door sales
5964	Direct Marketing - Catalog Merchants

### **Attachment 3 Continued**

5965	Direct Marketing -combination catalogue and retail merchants
5966	Direct Marketing - Outbound telemarketing
5967	Direct Marketing - Inbound telemarketing
5968	Direct Marketing - continuity subscription merchants
5969	Direct Marketing - Other Direct Marketers
5972	Stamp & coin stores
5993	Cigar stores & stands
6010	Manual Cash Disbursement **formerly Tours/Holiday/Vacations
6220	On Board Sales
7012	Timeshares
7276	Tax preparation Services
7297	Massage parlours
7542	Car washes
7631	Watch, Clock and Jewellery Repair Shops
7832	Motion picture cinemas
7932	Billiard & pool establishments
7933	Bowling alleys
7993	Video amusement game supplies
7994	Video game arcades and establishments
7996	Amusement Parks, Circuses, Carnivals and Fortune Tellers
8003	Movie Tickets

**Attachment 4**

<b>BLOCKED CATEGORIES (4)</b>	
<b>Merchant Number</b>	<b>Description</b>
7273	Dating and Escort Services
7995	Gambling Transactions Entertainment

**Enterprise Wide Defence Credit Cards Fraud Risk Assessment**  
*(Defence Travel Cards (DTC), Defence Purchasing Cards (DPC) and Cabcharge etickets)*

Date of Risk Review

September 2016

Group

CFOG

Division

Finance Business Information

Branch

Financial Services

Directorate/Unit/Project

Directorate of Financial Operations and Directorate of Financial Assurance and Compliance

Compiled by

Reviewed by

Endorsed by

Melinda Gabriel A/ASFB

David Spouse FASFS

Date of Next Review\*

Mar-17

Risk Identification			Control Assessment		Risk Assessment			Risk Evaluation and Treatment							DFAC Comments on Update		
Risk No.	Risk Description	Risk Cause	Directorate Controls	Control Owner	Control Effectiveness	Likelihood	Consequence	Risk Rating	Treatment Options	Proposed controls	Control Owner	Control Timeframes	Likelihood	Residual Consequence			
Assets and Inventory Financial																	
2.1	Fraudulent or Fraudulent and unauthorised use of a Defence credit card	Card holders who have left Defence not advising the Corporate Card Support Centre (CCSC) that their cards require cancelling.  Collusion between CMS supervisor and cardholder.  Card holders can dispute transactions to hide fraud.	Card Application Processing System (CAPS) initiates automatic cancellation of credit card based on daily matching of card holders against the daily feed from PMKeys employee data.	CFOG-FBI	Effective	Almost certain	Moderate	High	Reduce Likelihood & Consequence				Almost certain	Minor	Medium	As proposed during the March 2016 Reporting; the monthly manual cancellation of cards (for cardholders departing Defence) has been replaced with daily system automated cancellation.	
			This is a system initiated auto-cancellation of credit cards held by officials who have departed from Defence reduces the risk associated with ex-employees retaining active credit cards.														
			Annual QA (2.1.10) identifies purchase cards holders with a limit of over 250,000 to confirm if the high limit is still required (conducted during January).	CFOG- DFO	Effective												
			DFAC conducts monthly review of 100% credit card transactions for pre-defined high risk merchant categories and any unusual spending patterns are investigated.	CFOG- DFAC	Effective												
			Any credit card transactions not supported by adequate explanation are referred to Director Fraud Control	CFOG- DFAC	Partially Effective												
			Two merchant codes considered inappropriate have been blocked.	CFOG- DFO	Effective												
			Expenses are monitored by cost center managers.	All Staff	Partially Effective												
2.2	Unauthorised use of a Defence credit card	Opportunity for all Defence credit card holders or outsider to misuse their Defence Credit Card.  Weak or absent process  Lack Of understanding of Policy  Disregard for Policy  Absence of management oversight  Use of Defence credit card to purchase items for personal use.	Audit and Fraud Control Division conducts a targeted fraud detection program which includes credit cards.	FAS Audit and Fraud Control	Partially Effective	Almost certain	Moderate	High	Reduce Likelihood & Consequence				Almost certain	Minor	Medium	As proposed control during the March 2016 Reporting has been implemented.	
			DFAC conducts monthly review of 100% credit card transactions for pre-defined high risk merchant categories and any unusual spending patterns are investigated.	CFOG- DFAC	Partially Effective												
			Any credit card transactions not supported by adequate explanation are referred to Director Fraud Control	CFOG- DFAC	Partially Effective												
			CFOG-FBI has implemented a new work program to support detection of unauthorised use of credit card.	CFOG-FBI	Effective												
			All Credit Cards not activated within 90 days are cancelled.	CFOG- DFO	Effective												
			All physical Credit Cards are subject to unique pin codes.	CFOG- DFO	Effective												
			System alert has been implement to notify incoming and outgoing supervisors when change in supervisor occurs.	CFOG- DFO & Supervisors	Partially Effective												
			An automated email is sent to card holder and supervisor for any Credit card transactions are not acquitted by cardholder within 60 days of the transaction being recorded in Card Management System (CMS).	All Staff	Partially Effective												
			All new credit cards are issued with following default spending limits unless Group CFOs or their delegate approval is provided for any business case for higher spending limit:  Travel Card: \$10,000 Purchase Card: \$30,000 Virtual Card : \$500,000  CFOG-DFO has already implemented this control on all new credit cards. CFOG-DFO has reviewed and validated all existing DPC and DTC and where applicable the Group CFO have requested for cancellation or change of spending limit.	CFOG -DFO, All Staff for exceptions to default	Effective												
			Two person approval process: CMS prevents cardholders to accept their own transaction.	CFOG- DFO	Partially Effective												
CMS Supervisors are determined by the Group CFO or their delegate.	CFOG-ASFBI - DFO	Partially Effective	CMS acquittal is scheduled to be removed with automated transaction loads. CFOG-FBI will implement forensic, exception based reporting to mitigate the risk.	CFOG-FBI	15-Oct-16												
			CFOG will issue a cardholder list each January for review by Group CFOs.	CFOG- DFO	30-Jan-17												
			The Group CFO's (or their delegate) will annually review the following to determine whether to retain or alter: - Individual Credit Card spending limits - Individual Credit Card cash transferral limits - Virtual Credit Card limits - Unused Credit Cards	Group CFOs	30-Jan-17												

Risk No.	Risk Identification		Control Assessment			Risk Assessment			Risk Evaluation and Treatment							DFAC Comments on Update
	Risk Description	Risk Cause	Directorate Controls	Control Owner	Control Effectiveness	Likelihood	Consequence	Risk Rating	Treatment Options	Proposed controls	Control Owner	Control Timeframes	Likelihood	Residual Consequence	Risk Rating	
2.3	Unauthorised withdrawal of money using DPC.	Opportunity for card holders to withdraw cash from DPC  Cardholders can request for an increase in the credit card limit.	All requests to access cash through the DPC require Group CFO approval and FASRA sign off. A register of all requests is maintained and a QA is conducted annually (January) where card holders are asked if cash access is still required	Group CFOs CFOG- DFO	Partially Effective	Possible	Minor	Low	Retain the Risk by Informed Decision							The risk assessment has been updated to reflect implementation of proposed control during the March 2016 Reporting.
			All new DPC card have \$0 default cash transfer limit and any change to the default cash transfer limit for Purchasing Card requires approval of Group CFOs.	Group CFOs	Effective											
			All existing DPC limits have been reviewed, validated and where applicable request for cancellation or request for spending limit change have been made by the Group CFOs.	CFOG- DFO	Effective											
			DFAC reviews all DPC cash withdrawals and any travel card cash withdrawals over \$950.	CFOG-DFAC	Partially Effective											
			DPC cash withdrawals are reviewed monthly and any withdrawal without FASRA signoff are forwarded to Group CFO.	CFOG-DFAC	Partially Effective											
										CFOG will issue a cardholder list each January for review by Group CFOs.	CFOG- DFO	30-Jan-17				
										The Group CFO's (or their delegate) will annually review the Individual Credit Card cash transferral limits to determine whether to retain or alter.	Group CFOs	30-Jan-17				
2.4	Unauthorised withdrawal of money using DTC.	ATM cash withdrawals limit is set to \$1,000 per day however, Travelex outlets enable Card holders to withdraw larger amounts of money without approval.  Opportunity for card holders to withdraw cash from DTC.	Any request from Travelex of greater than \$10,000 requires Diners to obtain Group CFO approval. Cardholder is required to pre-inform and gain approval from the Group CFO.	CFOG-FBI	Effective	Likely	Minor	Medium	Reduce Consequence				Likely	Minor	Medium	The risk assessment has been updated to reflect implementation of proposed control during the March 2016 Reporting.
			All DTC card holder travelling overseas if needed are able to obtain approval for a companion MasterCard from their Group CFO 4 weeks prior to departure.	ALL	Partially Effective											
			All existing DTC limits have been reviewed, validated and where applicable request for cancellation or request for spending limit change have been made by the Group CFOs.	CFOG- DFO	Effective											
										CFOG will issue a cardholder list each January for review by Group CFOs.	CFOG- DFO	30-Jan-17				
										The Group CFO's (or their delegate) will annually review the Individual Credit Card cash transferral limits to determine whether to retain or alter.	Group CFOs	30-Jan-17				
2.5	Unauthorised person requesting a Defence credit card.	Anyone with DRN access has the ability to apply for a Defence credit card	A QA (verification of PMKeys and personnel data) upon receipt of applications to ensure that the applicant is a Defence official. (Supervisor approval of CMS access is required before Defence Credit Card is approved.)	CFOG-DFO	Effective	Unlikely	Moderate	Low	Reduce Consequence				Unlikely	Minor	Low	
			The revised (08/09/16) AE 602 Corporate Card Application and Limit Amendment requires : - Supervisor approval for application of DPC Card -Group CFO approval for application to change card limit (both DTC and DPC)	CFOG-DFO	Partially Effective											
2.6	Unauthorised opening of a Cabcharge account	Anyone with a Defence email can open a Cabcharge account and charge the account to Defence	All correspondence to Cabcharge from Defence officials is forwarded to central point of contracts within Defence for approval.	CFOG	Partially Effective	Possible	Moderate	Medium	Retain the Risk by Informed Decision							
2.7	Fraudulent use of Defence Cabcharge e-tickets	Lack of control and monitoring of Cabcharge e-tickets once they have been issued.	Units have local rules regarding the issuing and monitoring of Cabcharge e-tickets.	ALL	Partially Effective	Possible	Moderate	Medium	Reduce Likelihood & Consequence				Possible	Minor	Low	
										Usage and payment of Cabcharge e-tickets will be centrally managed and central register for Cabcharge e-tickets will be maintained in Sharepoint.	CFOG- DFO	30-Dec-16				
										Review of 280 eticket accounts is being undertaken to ensure proper management by the eticket account holders.	CFOG-DFAC	30-Dec-16				
2.8	Incorrect use of Cabcharge e-tickets	Cabcharge e-tickets are being issued to defence members instead of the member being directed to use DTC.	Customer Service Centres CSC issue Cabcharge e-tickets strictly in accordance with the type of travel.	ALL	Partially Effective	Almost certain	Moderate	High	Reduce Likelihood & Consequence				Possible	Minor	Low	
			DFAC has commenced a monthly review of Cabcharge expenses > 500.	CFOG-DFAC	Partially Effective											
										Monthly reconciliation of cabcharge accounts.	CFOG- DFO	15-Nov-16				
										Usage and payment of Cabcharge e-tickets will be centrally managed and central register for Cabcharge e-tickets will be maintained in Sharepoint.	CFOG- DFO	30-Dec-16				

SMART Principles
<b>Specific</b> Is the control clearly defined, consistent and unambiguous? Does the control identify a specific outcome?
<b>Measurable</b> Does the control provide timely, relevant, actionable and insightful information? Are there mechanisms in place to provide the information required to measure the effectiveness of the control?
<b>Achievable</b> Is operation of the control achievable? What events could affect the operation of the control? Is there an identified accountable position with ownership of the control?
<b>Relevant</b> Does the control serve to mitigate either the likelihood or the consequence of the risk being realised?
<b>Time-bound</b> Are there key timelines for operation of the control outlined?



## **Annex D Fuel Control Framework Current**

### **BUSINESS PROCESS TESTING FRAMEWORK**

#### **INTRODUCTION**

1. The internal audit function provides an independent and objective review to management that the designed financial and logistics controls are managing the organisation's risks and achieving their objectives. This also ensures that the Key Business Process Controls are operating in an efficient and effective manner as well as assisting management in improving organisational performance.
2. The evidence-based approach is used in audits to reach reliable and re-performable audit conclusions in a systematic audit process. Evidence will be collected on Key Business Process Controls for both preventive and detective controls.

#### **AIM**

3. The aim of this chapter is to describe the framework adopted by Defence Logistics Compliance and Assurance Network Teams to conduct Business Process Testing (BPT) and to outline the relevant testing standards, templates and reporting requirements that apply.

#### **AUTHORITY**

4. The ESCM is authorised jointly by the Secretary and the Chief of the Defence Force (CDF) IAW [DI\(G\) LOG 4-1-002](#).

#### **SCOPE**

5. The scope of this chapter is to state the BPT framework for the Defence Logistics Compliance and Assurance Network.

### **BUSINESS PROCESS TESTING FRAMEWORK**

6. The BPT is a means by which compliance and assurance with Defence supply chain policies and procedures is ascertained, and in conjunction with other control frameworks, is a part of the Defence Inventory Assurance Strategy (IAS). The BPT framework consists of the following elements that are described in more detail in subsequent paragraphs:

- a. High Impact Unit List.
- b. BPT Requirement and Frequency Determination.
- c. BPT Tool.
- d. BPT Reliance Key.

## **HIGH IMPACT UNIT LIST (FORMERLY HIGH MATERIALITY LIST)**

- 7. As part of the Defence Inventory Assurance Strategy, each year Logistics Assurance Branch (LAB) identifies Business Units that are likely to have a high impact on the accuracy of the Defence Asset and Inventory Accounts held in MILIS. This list is published annually as the High Impact Unit List (HIUL).
- 8. Factors taken into account when developing the HIUL are:
  - a. Value of Inventory and Assets held (or managed) by Business Units and System Project Offices (SPOs). This includes warehouse and SCA holdings.
  - b. BPM Results.
  - c. NAIS outcomes.
  - d. Most recent BPT result.
  - e. Stocktake results.
  - f. Input from key stakeholders.
- 9. Materiality for other Logistics Information Systems (LIS) will be selected from the respective Logistics Information Systems (eg SLIMS).

## **BPT REQUIREMENT AND FREQUENCY DETERMINATION**

- 10. BPTs are scheduled by financial year in conjunction with the Group or Service Tier 3. BPTs can also be included into the schedule/ when required by LAB and on request by AFCD or ANAO.
- 11. The frequency for the conducting a MILIS BPT at a BU is:
  - a. Business Units on the High Impact Unit List (HIUL);
    - 1. Within the current financial year.
  - b. Business Units that operate one or more MILIS warehouses:

1. Once every three years if the Business Unit has no more than four BPM red traffic lights on the same controls consecutively over three months; or
  2. If the Business Unit has five or more red BPM KPI traffic lights on the same controls consecutively over three months. A BPT is to be scheduled by T3 within 18 months of occurrence.
12. The requirement for a SLIMS BPT to be conducted is determined by the following:
- a. Major Fleet Units (MFUs) and Minor Warfare Vessels (MWVs) using SLIMS:
    1. MFUs and MWVs identified on the HIUL will be subject to a Departmental Management Audit (DMA) / BPT annually.
    2. MFUs or MWVs that are not on the HIUL with ongoing poor results will be considered by Director General Logistics – Navy (DGLOG–N), in consultation with the Executive Director Logistics Assurance (EDLA) as a high compliance and assurance risk, at which time they will be considered for inclusion on the HIUL and will be assessed annually.
    3. Where a MFU or MWV has received a BPT score of 50 percent or less and/or has eight or more CARs raised, the ship is to be notified that another abridged DMA focusing on logistics will be conducted within 9 months of the initial DMA. This DMA will be subject to availability and operational tasking of the MFU or MWV.

#### Note

*Where a MFU or MWV has not achieved a suitable standard, the additional logistics focused DMA will be an added audit impost. It is not required if the DMA and BPT for a ship is above the 50 percent BPT Key Performance Indicator (KPI) and below the eight CAR KPI. It is designed to serve as an incentive for the MFUs and MWVs to ensure compliance with logistics procedures.*

- b. The minimum frequency for SLIMS BPT/DMA is 2 years (excluding any time in refit or deep maintenance).

13. Where Business Units have multiple warehouses under their management, Groups and Services' Tier 3 are to determine if the BU is to be tested as a complete entity or the testing limited to specific warehouses that are considered to pose the highest risks. Groups and Services are to advise LAB of details when the option of limiting the BPT to specific warehouses has been selected.
14. BPTs for units on the High Impact Unit List or those triggered by BPM KPI breaches are to be tested against all processes applicable to the Business Unit.
15. The above frequency is the minimum requirement to meet an appropriate level of governance. Groups and Services are to conduct a risk assessment on their Business Units and can schedule more frequent BPTs if their risk assessment or internal procedures warrant. Factors that can be taken into account in the risk assessment include (but are not limited to):
  - a. Previous BPT Results.
  - b. BPM KPI results or trends.
  - c. Stocktake results.
  - d. NAIS or other audit results.
  - e. Staff turn-over or unit relocation
16. Groups and Services are to develop an annual Financial year BPT Schedule and advise details to LAB by 01 August each year. LAB staff will consolidate the individual schedules into an overall Defence schedule and advise details of LAB staff participation/observation in specific BPTs. Amendments to the Group and Service schedules are to be advised to LAB within one month of being identified.

## 17. BUSINESS PROCESS TESTING TOOL

18. C&A testing is conducted, and results recorded, using a structured BPT Tool. There are currently two formats of the BPT Tool available:
  - a. On-line BPT Tool – accessed from the [LAB DLPM BPT Webpage](#) or from the link in ESCM [V10S03C06](#). This format is currently used for MILIS and SLIMS.
  - b. Manual (Excel spreadsheet) BPT Tool – accessed from the relevant ESCM chapter in V10S03 and is currently used by Fuel Services and Explosive Ordnance Branches for JEFMS and COMSARM BPTs.
19. Both of these BPT tools comprise of three segments as follows:
  - a. Business Management Practices (BMP). The BMP segment of the BPT contains a list of the most important steps in a business process, omission of which would affect completion of the process. The BMP is conducted as a walk through of the business process with the unit representative to provide the auditor with an understanding of how the process is conducted at the site, to provide an understanding of any local variations and to identify if there are any significant steps that are being missed. The tester will use a range of tools to assist them to make an assessment. These can include physical evidence, reports, observations, discussions with staff and any previous BPT results.
  - b. Key Business Process Controls (BPC). These are controls within each of the business process segments that pose a significant financial or supply chain impact on the business process. Physical testing of transactions and reports is conducted to determine if the process is operating in accordance with the ESCM.
  - c. Business Management Controls (BMC). Testing of Management Reporting. This activity tests a range of system reports to determine if relevant action has been taken by the Business Unit to correct any transaction exceptions identified by the reports. (This section is replaced by a Business Process Monitoring (BPM) Dashboard for MILIS.

20. The BPT Tool has been designed to manage both Preventative and Detective controls within each of the Business Processes conducted at Business Units.

### **Preventive Controls**

21. Preventative controls are applied during the normal flow of logistics transactions to identify any breakdown in the business process being tested. This is to prevent occurrence of error or fraud that could lead to misstatement of General Stores Inventory (GSI) or Military Support Item (MSI) balances.

### **Detective Controls**

22. Detective controls are used to assist in identifying any process errors, data errors or faults, including procedural faults or miss appropriation of assets that may have occurred.

### **BPT Reporting**

23. BPTs have a Quality Assurance (QA) review by the Tier 3. When the QA is completed, the BPT is to be submitted to LAB within 10 working days of the BPT being conducted. Completed BPTs are to be submitted as follows:
  - a. On-line BPT Tool. Completed BPTs are to have their status updated to 'with LAB' and an electronic copy of completed sample sheets and supporting evidence for any non-compliances placed in the LAB objective folder for the Group or Service.
  - b. Manual BPT Tool. Electronic copies of completed manual BPT spreadsheets, completed sample sheets and supporting evidence for non-compliances are to be placed in the LAB objective folder for the Group or Service. The relevant BPT coordinator is to be advised of completion. NOTE: Manual BPTs are only to be used for JFMS and COMSARM systems.

## BPT RELIANCE KEY

24. A BPT Reliance Key is used by Defence to support measurement and reporting of compliance levels across Groups and Services. The key is used to report compliance levels for a BU at the conclusion of each BPT (via the Executive Summary Report) and at a summary level by process and Group or Service on a periodic basis. The threshold for BPT compliance is 85%.

Percentage	Level of Reliance
0.00% - 49.99%	No Reliance
50.0% - 74.99%	Low Reliance
75.0% - 84.99%	Moderate Reliance
85.0% - 100%	High Reliance

1. TABLE 1: BPT RELIANCE KEY

Control Activity	Role Responsible	Testing and Sampling Method
Ensure the Defence Fuel Card is maintained for the vehicle/asset.	Unit Transport Manager/SG Fleet	From the selected sample, the testing team is to verify the Defence Fuel Card is maintained for the vehicle/asset: <b>(1)</b> the correct Defence Fuel Card is allocated to the vehicle/asset, <b>(2)</b> any outstanding Exceptions over 30 days has an investigation in pro
Ensure the AD049 Vehicle Log is maintained for the vehicle/asset.	Unit Transport Manager	From the selected sample, the testing team is to verify the AD049 Vehicle Log is maintained for the vehicle/asset for the past 12 months, when the vehicle/asset was in use: <b>(1)</b> all the driver's details clear, coherent and all details completed in the AD04
The Waste Fuel Disposal Report is actioned on a monthly basis.	FSB LSA	The testing team is to undertake a DTR to validate the the oldest line within the following parameters: For Wholesale Units <ul style="list-style-type: none"> <li>- Between 30 - 90 days the score = 4 (GREEN) Compliant</li> <li>- Between 91 - 180 days the score = 2 (AMBER) Unit to remediate</li> </ul>
Aging Dispute Transaction (remain unresolved for more than 30 days from the date they were disputed) Report is actioned monthly.	FSB	The testing team is to undertake a DTR to validate the the oldest line within the following parameters: For Wholesale Units <ul style="list-style-type: none"> <li>- Between 30 - 90 days the score = 4 (GREEN) Compliant</li> <li>- Between 91 - 180 days the score = 2 (AMBER) Unit to remediate</li> </ul>
The Invalid ODO Reading Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0</li> </ul>

Control Activity	Role Responsible	Testing and Sampling Method
		(RED) Teir 3 / FSLAB to escalate to 1*.
The Excessive Fuel (Overfill) Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
The Recent Infringements Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
The Fuel Cards Being Used More Than 3 Times in a 24 Hr Period Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
The Inactive Fuel Cards Report is actioned and is completed.	Unit Transport Manager	The testing team is to undertake a DTR to validate the oldest line within the following parameters: <ul style="list-style-type: none"> <li>- Between 01 - 30 days the score = 4 (GREEN) Compliant</li> <li>- Between 31 - 60 days the score = 2 (AMBER) Unit to remediate</li> <li>- Greater than 60 days the score = 0 (RED) Tier 3/ FSLAB to escalate to 1*.</li> </ul>
Ensure the Annual Census was conducted and the results sent to SG Fleet.	Unit Transport Manager	The testing team is to validate when the last Annual Census was conducted. The testing team is to validate: <ol style="list-style-type: none"> <li>All Defence Fuel Cards were reconciled.</li> <li>Evidence of remediation for anomalies.</li> <li>Email confirmation to SG Fleet of completion of the Census</li> </ol>



## Merchant Codes Blocked as Inappropriate @ 5 Dec 2016

Source: Custom SQL from Promaster Audit table  
ObjectiveID: C:\DRMS Home\Objects\AF27596286.xls\CMS Table Data

Card Type	Merchant Type	Description	Merchant Group	Date Last Modified
ANZ Purchasing Card	7273	Dating and Escort Services	Blocked Merchant Code	17/10/2016
ANZ Purchasing Card	7995	Betting, Gambling Chips	Blocked Merchant Code	17/10/2016
ANZ Purchasing Card	1600	Real Estate Agent	Risky Transactions	NULL
ANZ Purchasing Card	1830	Traffic and Parking Fines	Risky Transactions	NULL
ANZ Purchasing Card	2110	Theatres & Ticket Services	Risky Transactions	NULL
ANZ Purchasing Card	3320	Furs	Risky Transactions	NULL
ANZ Purchasing Card	3500	Risky Transactions	Risky Transactions	NULL
ANZ Purchasing Card	3835	Duty Free	Risky Transactions	NULL
ANZ Purchasing Card	3844	Messenger Services	Risky Transactions	NULL
ANZ Purchasing Card	3856	In-Flight Sales	Risky Transactions	NULL
ANZ Purchasing Card	3882	Cheque Cashing	Risky Transactions	NULL
ANZ Purchasing Card	4400	Messenger Services	Risky Transactions	NULL
ANZ Purchasing Card	4722	Travel Agencies	Risky Transactions	5/12/2016
ANZ Purchasing Card	4723	Package Tour Operators (Germany Only)	Risky Transactions	5/12/2016
ANZ Purchasing Card	5094	W/Sale Precious Stones and Metals, Watches Jewelry	Risky Transactions	NULL
ANZ Purchasing Card	5193	W/Sale Florists Supplies, Nursery Stock and Flowers	Risky Transactions	NULL
ANZ Purchasing Card	5271	Mobile Home Dealers	Risky Transactions	NULL
ANZ Purchasing Card	5300	Wholesale Clubs	Risky Transactions	NULL
ANZ Purchasing Card	5309	Duty Free Stores	Risky Transactions	NULL
ANZ Purchasing Card	5592	Motor Home Dealers	Risky Transactions	NULL
ANZ Purchasing Card	5598	Snowmobile Dealers	Risky Transactions	NULL
ANZ Purchasing Card	5600	Inflight Sales	Risky Transactions	NULL
ANZ Purchasing Card	5681	Furriers and Fur Shops	Risky Transactions	NULL
ANZ Purchasing Card	5921	Bottled Liquor Sales, Hotel, Liquor Shops, Wineries	Risky Transactions	5/12/2016
ANZ Purchasing Card	5931	Used Merchandise Stores, Second Hand Stores	Risky Transactions	NULL
ANZ Purchasing Card	5932	Antique Shops	Risky Transactions	NULL
ANZ Purchasing Card	5933	Pawn Shops	Risky Transactions	NULL
ANZ Purchasing Card	5937	Antique Reproduction Stores	Risky Transactions	NULL
ANZ Purchasing Card	5944	Jewelry, Watches, Clocks, Silverware Stores	Risky Transactions	NULL
ANZ Purchasing Card	5948	Luggage and Leather Goods Stores	Risky Transactions	NULL
ANZ Purchasing Card	5960	Direct Marketing Insurance Services	Risky Transactions	NULL
ANZ Purchasing Card	5962	Telemarketing of Travel Related Arrangements	Risky Transactions	NULL
ANZ Purchasing Card	5963	Direct Selling Door to Door	Risky Transactions	NULL
ANZ Purchasing Card	5964	Catalog Merchants	Risky Transactions	5/12/2016
ANZ Purchasing Card	5965	Catalog and Retail Merchants Combined	Risky Transactions	5/12/2016
ANZ Purchasing Card	5966	Telemarketing Merchants - Outbound	Risky Transactions	NULL
ANZ Purchasing Card	5967	Inbound Teleservices Merchants	Risky Transactions	NULL
ANZ Purchasing Card	5968	Continuity/Subscription Merchants	Risky Transactions	5/12/2016
ANZ Purchasing Card	5969	Direct Marketers/Other	Risky Transactions	5/12/2016
ANZ Purchasing Card	5972	Stamps and Coin Stores	Risky Transactions	NULL
ANZ Purchasing Card	5993	Cigarette, Tobacconist Stores and Stands	Risky Transactions	NULL
ANZ Purchasing Card	6010	Bank Branches Cash Advances, Travellers Cheques	Risky Transactions	5/12/2016
ANZ Purchasing Card	6220	On-Board Sales	Risky Transactions	NULL
ANZ Purchasing Card	7012	Timeshares	Risky Transactions	NULL
ANZ Purchasing Card	7276	Tax Preparation Services	Risky Transactions	5/12/2016

## Merchant Codes Blocked as Inappropriate @ 5 Dec 2016

Source: Custom SQL from Promaster Audit table  
ObjectiveID: C:\DRMS Home\Objects\AF27596286.xls\CMS Table Data

Card Type	Merchant Type	Description	Merchant Group	Date Last Modified
ANZ Purchasing Card	7297	Massage Parlors	Risky Transactions	NULL
ANZ Purchasing Card	7542	Car Washes	Risky Transactions	5/12/2016
ANZ Purchasing Card	7631	Watch, Clock and Jewelry Repairs	Risky Transactions	NULL
ANZ Purchasing Card	7832	Motion Picture Theaters	Risky Transactions	NULL
ANZ Purchasing Card	7932	Billiard and Pool Saloons	Risky Transactions	NULL
ANZ Purchasing Card	7933	Bowling Alleys	Risky Transactions	NULL
ANZ Purchasing Card	7993	Video Game Supplies	Risky Transactions	NULL
ANZ Purchasing Card	7994	Video Game Arcades/Establishments	Risky Transactions	NULL
ANZ Purchasing Card	7996	Amusement Paadmin, Circuses, Carnivals, Fortune Tellers Etc	Risky Transactions	NULL
ANZ Purchasing Card	8003	Movie Tickets	Risky Transactions	NULL
ANZ Purchasing Card	9222	Fines	Risky Transactions	5/12/2016
Diners Travel Card	7273	Dating and Escort Services	Blocked Merchant Code	18/01/2016
Diners Travel Card	7995	Gambling Transactions Entertainment	Blocked Merchant Code	1/04/2016
Diners Travel Card	1600	Real Estate Agent	Risky Transactions	18/01/2016
Diners Travel Card	1830	Traffic and Parking Fines	Risky Transactions	18/01/2016
Diners Travel Card	2110	Theatres & Ticket Services	Risky Transactions	2/12/2016
Diners Travel Card	3320	Furs	Risky Transactions	18/01/2016
Diners Travel Card	3500	Duty Free	Risky Transactions	18/01/2016
Diners Travel Card	3835	Duty Free	Risky Transactions	1/04/2016
Diners Travel Card	3844	Messenger Services	Risky Transactions	18/01/2016
Diners Travel Card	3856	Inflight Sales	Risky Transactions	1/04/2016
Diners Travel Card	3882	Cheque Cashing	Risky Transactions	1/04/2016
Diners Travel Card	4400	Messenger Services	Risky Transactions	18/01/2016
Diners Travel Card	4722	Travel Agencies and Tour Operators	Risky Transactions	1/04/2016
Diners Travel Card	4723	Package Tour Operators (Germany Only)	Risky Transactions	18/01/2016
Diners Travel Card	5094	Precious Stones, Metals, Watches & Jewellery	Risky Transactions	18/01/2016
Diners Travel Card	5193	Florists Supplies, Nursery Stock and Flowers	Risky Transactions	18/01/2016
Diners Travel Card	5271	Mobile Home Dealers	Risky Transactions	18/01/2016
Diners Travel Card	5300	Wholesale Clubs	Risky Transactions	18/01/2016
Diners Travel Card	5309	Duty Free Shops	Risky Transactions	1/04/2016
Diners Travel Card	5592	Motor Home Dealers	Risky Transactions	18/01/2016
Diners Travel Card	5598	Snowmobile Dealers	Risky Transactions	18/01/2016
Diners Travel Card	5600	Inflight Sales	Risky Transactions	18/01/2016
Diners Travel Card	5681	Furriers and Fur Shops	Risky Transactions	1/04/2016
Diners Travel Card	5921	Package Stores, Beer, Wine, and Liquor	Risky Transactions	5/12/2016
Diners Travel Card	5931	Used Merchandise and Secondhand Stores	Risky Transactions	18/01/2016
Diners Travel Card	5932	Antique Stores	Risky Transactions	18/01/2016
Diners Travel Card	5933	Pawn Shops	Risky Transactions	18/01/2016
Diners Travel Card	5937	Antique Reproductions	Risky Transactions	18/01/2016
Diners Travel Card	5944	Clock, Jewelry, Watch, and Silverware Store	Risky Transactions	1/04/2016
Diners Travel Card	5948	Leather Goods and Luggage Stores	Risky Transactions	1/04/2016
Diners Travel Card	5960	Direct Marketing Insurance Services	Risky Transactions	18/01/2016
Diners Travel Card	5962	Direct Marketing - Travel Related Arrangement Services	Risky Transactions	18/01/2016
Diners Travel Card	5963	Door-To-Door Sales	Risky Transactions	18/01/2016
Diners Travel Card	5964	Direct Marketing - Catalog Merchants	Risky Transactions	18/01/2016

## Merchant Codes Blocked as Inappropriate @ 5 Dec 2016

Source: Custom SQL from Promaster Audit table  
ObjectiveID: C:\DRMS Home\Objects\AF27596286.xls\CMS Table Data

Card Type	Merchant Type	Description	Merchant Group	Date Last Modified
Diners Travel Card	5965	Direct Marketing — Combination Catalogue and Retail Merchants	Risky Transactions	18/01/2016
Diners Travel Card	5966	Direct Marketing - Outbound Telemarketing	Risky Transactions	18/01/2016
Diners Travel Card	5967	Direct Marketing - Inbound Telemarketing	Risky Transactions	18/01/2016
Diners Travel Card	5968	Direct Marketing — Continuity/Subscription Merchants	Risky Transactions	18/01/2016
Diners Travel Card	5969	Direct Marketing - Other Direct Marketers	Risky Transactions	18/01/2016
Diners Travel Card	5972	Stamp & Coin Stores	Risky Transactions	18/01/2016
Diners Travel Card	5993	Cigar Stores & Stands	Risky Transactions	18/01/2016
Diners Travel Card	6010	Manual Cash Disbursement	Risky Transactions	1/04/2016
Diners Travel Card	6220	On Board Sales	Risky Transactions	18/01/2016
Diners Travel Card	7012	Timeshares	Risky Transactions	18/01/2016
Diners Travel Card	7276	Tax Preparation Services	Risky Transactions	18/01/2016
Diners Travel Card	7297	Massage Parlours	Risky Transactions	18/01/2016
Diners Travel Card	7542	Car Washes	Risky Transactions	18/01/2016
Diners Travel Card	7631	Watch, Clock, and Jewellery Repair Shops	Risky Transactions	18/01/2016
Diners Travel Card	7832	Motion Picture Cinemas	Risky Transactions	18/01/2016
Diners Travel Card	7932	Billiard & Pool Establishments	Risky Transactions	18/01/2016
Diners Travel Card	7933	Bowling Alleys	Risky Transactions	18/01/2016
Diners Travel Card	7993	Video Amusement Game Supplies	Risky Transactions	18/01/2016
Diners Travel Card	7994	Video Game Arcades and Establishments	Risky Transactions	18/01/2016
Diners Travel Card	7996	Amusement Parks, Circuses, Carnivals, and Fortune Tellers	Risky Transactions	18/01/2016
Diners Travel Card	8003	Movie Tickets	Risky Transactions	18/01/2016
Diners Travel Card	9222	Fines	Risky Transactions	1/04/2016
NAB Purchasing Card	7273	Dating and Escort Services	Blocked Merchant Code	18/01/2016
NAB Purchasing Card	7995	Betting, Gambling Chips	Blocked Merchant Code	18/01/2016
NAB Purchasing Card	1600	Real Estate Agent	Risky Transactions	NULL
NAB Purchasing Card	1830	Traffic & Parking Fines	Risky Transactions	NULL
NAB Purchasing Card	2110	Theaters & Parking Fines	Risky Transactions	NULL
NAB Purchasing Card	3320	Furs	Risky Transactions	NULL
NAB Purchasing Card	3500	Duty Free	Risky Transactions	NULL
NAB Purchasing Card	3835	Duty Free	Risky Transactions	NULL
NAB Purchasing Card	3844	Messenger Services	Risky Transactions	NULL
NAB Purchasing Card	3856	In-Flight Sales	Risky Transactions	NULL
NAB Purchasing Card	3882	Cheque Cashing	Risky Transactions	NULL
NAB Purchasing Card	4400	Messenger Services	Risky Transactions	NULL
NAB Purchasing Card	4722	Travel Agencies	Risky Transactions	19/01/2016
NAB Purchasing Card	4723	Package Tour Operators (Germany Only)	Risky Transactions	18/01/2016
NAB Purchasing Card	5094	W/Sale Precious Stones and Metals, Watches Jewelry	Risky Transactions	18/01/2016
NAB Purchasing Card	5193	W/Sale Florists Supplies, Nursery Stock and Flowers	Risky Transactions	18/01/2016
NAB Purchasing Card	5271	Mobile Home Dealers	Risky Transactions	18/01/2016
NAB Purchasing Card	5300	Wholesale Clubs	Risky Transactions	18/01/2016
NAB Purchasing Card	5309	Duty Free Stores	Risky Transactions	18/01/2016
NAB Purchasing Card	5592	Motor Home Dealers	Risky Transactions	18/01/2016
NAB Purchasing Card	5598	Snowmobile Dealers	Risky Transactions	18/01/2016
NAB Purchasing Card	5600	Inflight Sales	Risky Transactions	NULL
NAB Purchasing Card	5681	Furriers and Fur Shops	Risky Transactions	18/01/2016

## Merchant Codes Blocked as Inappropriate @ 5 Dec 2016

Source: Custom SQL from Promaster Audit table  
ObjectiveID: C:\DRMS Home\Objects\AF27596286.xls\CMS Table Data

Card Type	Merchant Type	Description	Merchant Group	Date Last Modified
NAB Purchasing Card	5921	Bottled Liquor Sales, Hotel, Liquor Shops, Wineries	Risky Transactions	5/12/2016
NAB Purchasing Card	5931	Used Merchandise Stores, Second Hand Stores	Risky Transactions	18/01/2016
NAB Purchasing Card	5932	Antique Shops	Risky Transactions	18/01/2016
NAB Purchasing Card	5933	Pawn Shops	Risky Transactions	18/01/2016
NAB Purchasing Card	5937	Antique Reproduction Stores	Risky Transactions	18/01/2016
NAB Purchasing Card	5944	Jewelry, Watches, Clocks, Silverware Stores	Risky Transactions	18/01/2016
NAB Purchasing Card	5948	Luggage and Leather Goods Stores	Risky Transactions	18/01/2016
NAB Purchasing Card	5960	Direct Marketing Insurance Services	Risky Transactions	18/01/2016
NAB Purchasing Card	5962	Telemarketing of Travel Related Arrangements	Risky Transactions	18/01/2016
NAB Purchasing Card	5963	Direct Selling Door to Door	Risky Transactions	18/01/2016
NAB Purchasing Card	5964	Catalog Merchants	Risky Transactions	18/01/2016
NAB Purchasing Card	5965	Catalog and Retail Merchants Combined	Risky Transactions	18/01/2016
NAB Purchasing Card	5966	Telemarketing Merchants - Outbound	Risky Transactions	18/01/2016
NAB Purchasing Card	5967	Inbound Teleservices Merchants	Risky Transactions	18/01/2016
NAB Purchasing Card	5968	Continuity/Subscription Merchants	Risky Transactions	18/01/2016
NAB Purchasing Card	5969	Direct Marketers/Other	Risky Transactions	18/01/2016
NAB Purchasing Card	5972	Stamps and Coin Stores	Risky Transactions	18/01/2016
NAB Purchasing Card	5993	Cigarette, Tobacconist Stores and Stands	Risky Transactions	18/01/2016
NAB Purchasing Card	6010	Bank Branches Cash Advances, Travellers Cheques	Risky Transactions	18/01/2016
NAB Purchasing Card	6220	On-Board Sales	Risky Transactions	NULL
NAB Purchasing Card	7012	Timeshares	Risky Transactions	18/01/2016
NAB Purchasing Card	7276	Tax Preparation Services	Risky Transactions	18/01/2016
NAB Purchasing Card	7297	Massage Parlors	Risky Transactions	18/01/2016
NAB Purchasing Card	7542	Car Washes	Risky Transactions	18/01/2016
NAB Purchasing Card	7631	Watch, Clock and Jewelry Repairs	Risky Transactions	18/01/2016
NAB Purchasing Card	7832	Motion Picture Theaters	Risky Transactions	18/01/2016
NAB Purchasing Card	7932	Billiard and Pool Saloons	Risky Transactions	18/01/2016
NAB Purchasing Card	7933	Bowling Alleys	Risky Transactions	18/01/2016
NAB Purchasing Card	7993	Video Game Supplies	Risky Transactions	18/01/2016
NAB Purchasing Card	7994	Video Game Arcades/Establishments	Risky Transactions	18/01/2016
NAB Purchasing Card	7996	Amusement Parks, Circuses, Carnivals, Fortune Tellers Etc	Risky Transactions	18/01/2016
NAB Purchasing Card	8003	Movie Tickets	Risky Transactions	NULL
NAB Purchasing Card	9222	Fines	Risky Transactions	5/12/2016



**Australian Government**  
**Department of Defence**



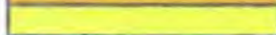
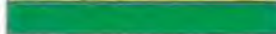
**Summary**  
**Control Effectiveness Testing Report**  
**Round 1**  
**2014-15**

**Overall Risk Rating**



Group Finance Officer attention required. Some minor issues have been identified. If not addressed, have the potential over time to lead to some financial loss and/or reputational damage. The issues identified pose minor threats to Defence In-Being, Investment Program, Workforce, Strategic Reform, Compliance and/or Security Vetting Agency.

**KEY: Overall Risk Rating**

	Serious control deficiencies have been identified.
	Some major issues have been identified
	Some minor issues have been identified
	No major issues were identified

**Prepared by Audit Branch**  
**Audit & Fraud Control Division**

## Summary

### Control Effectiveness Testing Report Round 1, 2014-15

---

#### Objective and Methodology

The objective was to test the financial controls contained in the Defence Financial Risk Controls Framework (the Framework), owned and managed by the Chief Finance Officer Group (CFOG).

A key change to the Defence Financial Policy Framework involved the replacement of the Financial Management and Accountability Act (FMA) with the Public Governance, Performance and Accountability Act (PGPA) with effect from 1 July 2014.

The focus of this testing round was on financial delegations after the introduction of the PGPA Act for transactions occurring between 1 July 2014 and 30 September 2014.

#### Key Issues

For Round 1, 2014-15 nine individual controls were tested, with three being Financial Compliance controls and six being the related legacy Foundation controls. These controls were tested across the Groups/Services with 117 control tests performed, comprising a total of 2,697 individual samples tested (an increase of 150% over the number of samples tested in total for 2013-14), with the following results:

- 35 (30%) Fully Effective
- 18 (15%) Substantially Effective
- 57 (49%) Ineffective
- 7 (6%) Unable to be Tested

During the testing, 126 Certificate of Compliance (CoC) breaches were identified, representing 4.7% of the total samples tested and 610 Internal Defence Policy breaches were identified, representing 22.6% of the total samples tested.

The 126 CoC breaches identified in Round 1, 2014-15 comprised:

- 116 (92%) breaches relating to exercising of Financial Delegation with no record of delegation or delegation exceptions;
- 10 (8%) breaches of other Controls relating to AusTender publishing timeframe (3), no tax invoice (6), and absence of Defence Manager approval for overseas travel (1).

The 610 Internal Defence Policy breaches identified in Round 1, 2014-15, comprised:

- 269 (44%) breaches of Accounting Authority Instruction (AAI) 1.5.1.9 resulting from documentation provided to Audit Branch in a manner, incomplete documentation provided or documentation not provided at all.
- 341 (56%) breaches of other Internal Defence Policy relating to professional competencies (135), AusTender publishing (26) and incomplete or incorrectly completed Defence Card and related documentation (180).

If the AAI 1.5.1.9 breaches are excluded (relating to provision of information), the results are:

- 40 (34%) Fully Effective
- 21 (18%) Substantially Effective
- 49 (42%) Ineffective
- 7 (6%) Unable to be Tested

#### Overall Conclusion

The overall result is that the intention of the control was met for 45% of the controls tested and rated as Fully Effective or Substantially Effective, with 49% of controls being Ineffective. The remaining 6% were unable to be tested.

If the 269 breaches of AAI 1.5.1.9 are excluded, the result is that the intention of the control was met for 52% of the controls tested and rated as Fully Effective or Substantially Effective, with 42% of controls being Ineffective. The remaining 6% were unable to be tested.

DIRECTORATE OF FINANCIAL ASSURANCE AND COMPLIANCE

# Credit Card and Defence Financial Risk Controls Framework

---

Work plan for 2016-17

**Last updated 12 October 2016**

## Document Controls and Approvals

<b>Document Location</b>	Object ID: R27521039
--------------------------	----------------------

<b>Amendment History</b>	<b>Date</b>	<b>Version No</b>	<b>Amendment Details</b>

<b>Distribution</b>	<b>Defence</b>	<b>Position</b>	<b>Date of issue</b>



## Contents

Team Overview .....	3
Staffing .....	3
Credit Cards.....	4
Background .....	4
Intended outcomes.....	4
Determining what to test.....	4
Testing and sampling .....	5
Current .....	5
Limitations.....	5
Future.....	5
Evidence and assessment .....	6
Continuous improvement.....	7
Defining success.....	7
Test relevance and validity .....	7
New and extended tests .....	7
Financial Risk and Controls .....	8
Purpose .....	8
Update and maintenance .....	8
Initial consolidation/review .....	8
Ongoing rationalisation/simplification .....	8
Continuous review and improvement .....	10
Success criteria.....	10
Attachment A – Proposed work schedule .....	11
Attachment B – Proposed Defence Purchasing and Travel Card Tests.....	12
Attachment C – Defence Financial Risk Map 2015-16.....	13

## Team Overview

There are two distinct main responsibilities for the team: analysis and testing of credit card expenditure data and the maintenance and management of the Defence Financial Controls Framework.

An outcome view of all work undertaken is a key priority for the team, regardless of the task – there must be a genuine purpose and use for performing the work, the outcomes achieved must be assessed against these goals, and continuous improvement and feedback must become routine.

Credit card transaction analysis and testing is performed to provide assurance that expenditure is appropriate and legitimate, and complies with relevant legislation and policies. Shaping and altering behaviours, ensuring effective and appropriate policy and controls, and forecasting future trends and identifying emerging areas of concern or weakness are value-add outcomes intended from this work.

Management and maintenance of the Defence Financial Risk and Controls Matrix will initially focus on continuing work to streamline, simplify and consolidate those controls listed. The ongoing review and maintenance effort will seek to identify more effective and efficient controls and to ensure accurate assessment of the risks being controlled.

An overarching goal will be to seek automated system based controls and testing, taking advantage of current and future information sources. This should include engaging with the ERP project on requirements needed and capabilities that will become available.

## Staffing

The team currently consists of three staff, one part time, with a linear reporting structure. The scope of work to be performed within the overall area of responsibility will be determined based on order of priority set by management and the availability of resources.

Responsibilities within the team will be allocated with consideration given to: promoting learning and development opportunities, providing work of interest at a suitable level, and allowing ownership of specific tasks. An indicative weekly schedule of tasks is included as Attachment A.

Name	Level	Availability	Primary responsibility
Terence Smith	EL1	Fulltime	Controls and testing strategy; policy and control change proposals; escalation and investigation
Usha Pun	APS 6	Fulltime	Assess evidence and documentation, identifying gaps/weaknesses in controls and policy; monitor escalation and investigation triggers; SOD rules
Sabrina Zhang	APS 5	3 days per week	Test workbook updates; manage and issue information requests; update policy/legislation and process changes in RACM and SOPs

## Credit Cards

### Background

In October 2015 DFAC commenced business intelligence and data analysis to support the Defence Financial Control Framework.

This body of the work was initiated with investigation at the general ledger account level for transaction miscoding. The results of the investigation led to the expansion of the number of general ledger accounts, the monitoring of high-risk merchant categories and other potential fraud-related transactions.

CFO appointed a contractor (Deloitte) in early 2016 to provide assistance in further identifying, developing and enhancing the financial assurance testing program. Their work suggested, among other things, a number of tests based on Defence credit card data.

### Intended outcomes

At a high level, credit card transaction analysis and testing provides assurance to CFO that expenditure is appropriate and legitimate, and complies with relevant legislation and policies. This inherently acts as a measure of the effectiveness of controls.

The additional value-add from this work could reduce credit card expenditure and improve transparency, governance and compliance, by:

- Influencing changes in behaviour and expenditure
- Forecasting expenditure trends to improve test benchmarks
- Identifying emerging areas of concern to direct future testing
- Assessing any gaps and weaknesses in existing policies and controls

### Determining what to test

The initial set of tests requiring credit card data were suggested by CFO appointed contractor, Deloitte. Of the 39 'forensic' tests suggested, 18 related to credit cards, addressing cash advances, general misuse and travel related expenditure (Attachment B).

Further testing requirements are developing as a result of changes to the financial systems landscape, necessitating increased checks and assurance. The most current change introducing risk into credit cards and requiring an increased level of assurance and monitoring is the planned removal of CMS Supervisor roles.

CFO priorities and audit report findings will necessarily steer the direction for additional or modified analysis and testing program requirements.

It is also expected continuous improvement and feedback from within the team and externally will help refine and shape testing. Accepting and implementing feedback into the work program is vital to ensuring tests remain appropriate, effective and efficient.

## Testing and sampling

### Current

Testing is performed on the entire data set of previous month CMS data (average 157,552 records, ranging 70,213 – 184,776 per month in 2015/16), which is provided directly to the team at the beginning of each following month by the CMS administrators. This data is taken directly from the CMS database using a custom query to meet the requirements for the current and foreseeable testing of credit card transactions.

This data is inserted into the Excel 2010-based testing and analysis tool, with a series of Pivot tables providing complete and summary results (such as top 10) for each defined test. The testing and analysis workbook has been designed to be as easy as possible to use, and includes clear step by step instructions on the first tab.

Of the 18 proposed credit card related tests, 13 are currently being performed with the available data – including all cash advance and travel related tests originally proposed by the contractor (Attachment B).

### Limitations

Data volume, system integration and software limitations have shaped the current testing approach. These limitations have reduced responsiveness, necessitated reliance on other areas, and have prevented some tests from being performed.

- Due to the volume of data each month (average 157,552 rows per month in 2015/16), it is unable to be independently sourced by the team from BORIS, thus creating a reliance on the CMS administrator to extract and supply the data each month
- Due to the volume of data, the standard Defence desktop version of Excel 2003 was unable to be used, necessitating the installation and configuration of Excel 2010 on any desktop workstations being used by staff requiring access to the tool
- Timeliness and responsiveness is severely impacted by the current monthly data extraction and analysis process
  - results will be lagging by about 2-5 weeks from the date a transaction occurred
  - large peaks and troughs in staff workload that need to be managed
  - reduction in the potential ongoing educative benefits from assurance of transactions

### Future

#### *CMS supervisor*

With the imminent removal of the requirement for CMS Supervisors to approve transactions in the CMS system, it has been directed that additional tests need to be developed to provide assurance over the transactions. One of these is a commitment to test every card at least once per year. This will add significant workload and require additional resources and support.

#### *Corporate system solution*

If limitations outlined above are addressed, enabling automated real-time and near real-time testing within an integrated system solution, realised benefits could include:

- Suspicious transactions and breaches of controls can be automatically reported to staff, allowing immediate investigation and responsiveness to issues
  - Improved responsiveness should have a greater influence on behaviour
  - Improved timeliness of investigations would be likely to reduce financial loss
  - Automatic, real-time or near real-time testing would smooth out work cycles and allow more efficient staff structures
- System solution would provide multiple user access for the team to manage testing, controls and investigation of issues
- An integrated system solution with system interfaces to corporate data sources would reduce manual processes and minimise the risk of introducing errors into the data
- An official system solution would have the advantages of system support and backups, and a more easily identified and mapped plan for integration and migration to the new ERP

### *Replace existing reports*

The Systems team produce monthly summary reports showing the top transactions for a number of merchant categories. The provided workbook does not provide detail to enable investigation directly, requiring requests back to the Systems team before the data can be used for any testing purposes. The work effort on Colin's team to produce these reports is understood to be significant.

Within DFAC, there may be some overlap between the sampling and assurance activities managed by Sandra Cole and Michael Sharp and the output and testing performed by the credit card testing workbook.

In each of the above instances, where possible, it could be beneficial to use the data already sourced directly from CMS for the credit card workbook to produce these outputs/reports also. For example, the top 10 by merchant category for credit card expenditure should be easily incorporated directly into the workbook, thereby removing the burden from the systems team, and improving DFAC autonomy and self-sufficiency.

### **Evidence and assessment**

Transactions identified as requiring investigation/analysis as a result of testing will be followed up in a consistent and professional manner:

- Supporting documentation is sourced. The team will attempt to locate this information directly if it is available, otherwise a request will be sent to the card holder and/or account holder to provide the relevant documentation.
  - Typically required documentation would include travel budget calculators, receipts, and any documents that explain or justify the expenditure such as a signed Minute.
- Documentation is then assessed against the expenditure approval, appropriate internal policy, legislation, and appropriateness and expected standards.

If the requested documentation is not provided within a defined period of time (to be defined) due to relevant card holder or account holder refusing to cooperate, or because they do not respond at all, the issue will be escalated.

- FASFS or CFO to review justification to escalate, and if approved, the matter is forwarded to the relevant Group CFO to follow up.

- If there continues to be no resolution, FASFS or CFO to authorise matter to be forwarded to fraud for investigation.

Once all the information has been received and assessed, a judgement needs to be made.

- If the expenditure has all necessary approvals, adheres to regulations and policies, and appears to be appropriate – no further action is taken.
- If the expenditure has the required approvals and does not breach any policies, but appears not to be an appropriate or expected use of resources – review and feedback into policy and or controls to address potential gap.
- If the expenditure is in breach of approvals, legislation, policy or internal controls – forwarded to fraud for investigation.

### **Continuous improvement**

Ongoing review and assessment of the testing program is important to ensure it continues to provide value, continues to meet required outcomes, and is achieving the intended outcomes.

### **Defining success**

For every test, the intended outcome(s) and success criteria will be clearly defined and articulated prior to the test commencing. It is expected the outcomes will include, but not be limited to those listed under 'Intended Outcomes' above.

The success criteria against which the test will be assessed will be test specific and measurable, and will relate specifically to whether the test is achieving its intended outcome(s). For example, if the intention is to reducing instances of particular transactions, the assessment would look at whether there is a downwards trend in the instances of these transactions occurring.

### **Test relevance and validity**

If a test appears to fail to meet its objectives, an assessment is needed to determine whether this is due to the test definition (perhaps the wrong benchmark is being used) or whether the test design or follow up action is ineffective. Appropriate action will then be taken to address the weakness.

A further assessment of all tests, whether considered effective or not, is whether the test remains a requirement at all. Management decisions, system changes or policy/legislation updates may render some tests redundant. In this case, the test should cease immediately unless there is a compelling reason otherwise.

These assessments will be performed as a combination of formal reviews and based on experience and feedback from the team. The goal is to embed feedback and continuous improvement into the work plan and not to stifle innovation or responsiveness.

### **New and extended tests**

It is expected the number and content of tests will increase as the function matures and proves itself and processes become streamlined to support increased testing. This will also be dependent on having sufficient people available to conduct the work.

Feedback from within the Directorate, i.e. Sandra and Michael noticing trends or issues of interest, management direction, system changes and updates to policy and legislation will help define and shape ongoing testing innovations and improvements.

## Financial Risk and Controls

### Purpose

The development of the Defence Financial Risk Controls Framework (the Framework) is consistent with the AS/NZS ISO 31000:2009 *Risk Management Principle and Guidelines*, with the team specifically focused on monitoring and reporting the key controls that mitigate risk.

The purpose of these activities is to provide objective assurance to the most senior Defence management and the Defence Audit and Risk Committee on the effectiveness of key financial controls, and through this, a view on the overall financial health of Defence.

While discharging its responsibilities regarding the Framework, the team will also work to simplify and rationalise the Framework to ensure it is clear and concise and within reach of any employee to understand and apply, not just those with detailed knowledge and experience.

### Update and maintenance

#### Initial consolidation/review

Management and maintenance of the Framework will initially focus on finalising previously commenced work to consolidate the Defence and DMO (now CASG) risks and controls into a single document, and to update references to the *Financial Management and Accountability Act 1997* (Cth) and other superseded or repealed legislation and policy.

The initial review and consolidation will also identify Defence organisational references that are no longer valid, including positions and groups, updating those references where possible.

#### Ongoing rationalisation/simplification

The ongoing review and maintenance of the Framework will focus on ensuring its currency, completeness and effectiveness, by:

- Ensuring understanding and assessment of how the risks identified in the Defence Financial Risk Map (Attachment C) are realised
- Assessing the effectiveness of the controls implemented to mitigate the risks identified in the Defence Financial Risk Map
- Rationalising and redesigning existing controls, or implementing new controls, as appropriate to ensure an efficient and simplified set of controls

#### Understanding the risks

The Defence Finance Risk Map is reviewed annually and is consistent with the CFO's responsibilities under the Defence Enterprise Risk map as the steward for finance.

The key financial business risk areas identified are:

- Cash Flow / Budget Risk
- Financial Performance
- Financial Reporting
- Financial Compliance
- Financial Capability

In order to assess the effectiveness and efficiency of controls, it is vital to understand the risks they have been implemented to mitigate. This involves understanding each risk, including its:

- causes – how the risk is realised
- consequences – the severity and likelihood
- controls – current and best practice

In addition to the risks from the Defence Finance Risk Map, the team will seek to identify other risks that may result from internal processes, legislative requirements and technology changes.

#### *Understanding and assessing existing controls*

The approach initially will be to understand the risk and control landscape using detailed mapping of functions and/or processes. These maps will provide visual summaries (supported by detailed explanations) of where and how risks have been identified as being likely to be realised, and where and how in the relevant process the controls operate.

Of specific interest will be identifying through this mapping process which risks or controls are:

- manual or automated
- in-system or offline
- currently operating or listed against processes/activities no longer being performed

This mapping task will also seek to identify risks that have no identified controls, as well as those risks with multiple controls.

Identifying who (position or role) 'owns' a control and risk will assist ongoing maintenance of controls and risk assessments.

#### *Separation of Duties*

While a subset of overall system controls, the current review of the Separation of Duties (SOD) matrix requires a high level of knowledge of systems and controls, and is consuming significant resources due to the size of the current SOD list. As such, this is currently a focus in its own right.

Consistent with the overall review and assessment of the controls landscape, all SODs will be mapped to a specific identified risk. Where a risk is not identifiable, assessment as to the continued requirement for the SOD will be undertaken.



## Continuous review and improvement

### *Rationalise and simplify controls*

Once the mapping and consolidation work has been completed, the biggest ongoing value-add of the team will be to rationalise, streamline and simplify the controls, and to suggest improved business processes to improve the efficiency and effectiveness of the risk and control landscape.

Specifically, the team will use the initial and ongoing review of risks and controls to:

- identify and address control gaps and duplication
- incorporate industry best practice (insofar as it applies to our business)
- redesign and replace manual and offline controls with automated system solutions
- propose process/function changes to minimise risk realisation and to reduce and simplify required controls – ensuring the business outcomes can still be delivered

### *Success criteria*

Establishing clear success criteria to support objective assessment of the team's work in this area is vital to demonstrating value to the organisation. While the task to manage and maintain the Defence Financial Risk Controls Framework is difficult able to quantitatively measure, it is proposed we will assess the following outcomes:

- Risk ratings should reduce due to lower probability of the risk being realised
- Instances of risks actually being realised should be reduced
- Defence Financial Risk Controls Framework should be shorter and simpler
- Reduced/eliminated audit (internal or ANAO) findings relating to risk or controls

The overarching intent of establishing the above process for the maintenance of the risk and controls landscape is to support a program of ongoing incremental change, avoiding the need for disruptive wholesale changes.

*Terence Smith CPA*

*Assistant Director Financial Assurance and Compliance*

*P: 02 626 59182*

*E: [terence.smith2@defence.gov.au](mailto:terence.smith2@defence.gov.au)*

Attachment A – Proposed work schedule

Attachment B – Proposed Defence Purchasing and Travel Card Tests

Attachment C – Defence Financial Risk Map 2015-16

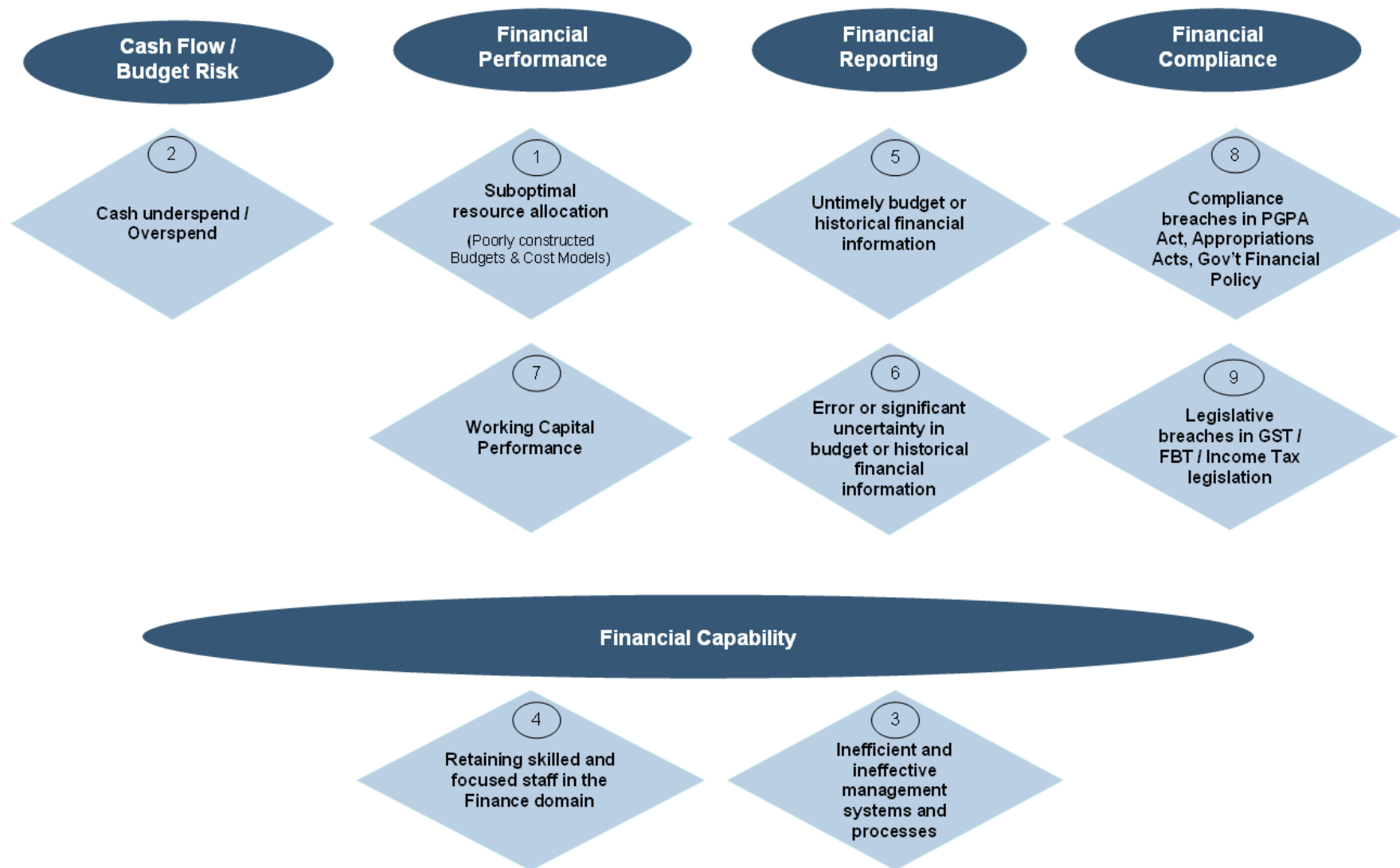
## Attachment A – Proposed work schedule

	Monday	Tuesday	Wednesday	Thursday	Friday
<b>Terence</b>	<ul style="list-style-type: none"> <li>Review 2<sup>nd</sup> level esc report</li> </ul>	<ul style="list-style-type: none"> <li>Esc to CFOs</li> <li>Fwd for investigation</li> </ul>	<ul style="list-style-type: none"> <li></li> </ul>	<ul style="list-style-type: none"> <li></li> </ul>	<ul style="list-style-type: none"> <li>Review weekly reports on testing</li> <li>Define testing changes for following week</li> </ul>
	<ul style="list-style-type: none"> <li>Overview process, control and risk</li> <li>Policy / system / control changes and improvements</li> </ul>	<ul style="list-style-type: none"> <li>Overview process, control and risk</li> <li>Policy / system / control changes and improvements</li> </ul>	<ul style="list-style-type: none"> <li>Overview process, control and risk</li> <li>Policy / system / control changes and improvements</li> </ul>	<ul style="list-style-type: none"> <li>Overview process, control and risk</li> <li>Policy / system / control changes and improvements</li> </ul>	<ul style="list-style-type: none"> <li>Overview process, control and risk</li> <li>Policy / system / control changes and improvements</li> </ul>
<b>Usha</b>	<ul style="list-style-type: none"> <li>Review 1<sup>st</sup> level esc report</li> <li>Advise 2<sup>nd</sup> level esc</li> </ul>	<ul style="list-style-type: none"> <li>send supervisor escalation</li> <li>Assess docs</li> </ul>	<ul style="list-style-type: none"> <li>Assess docs</li> </ul>	<ul style="list-style-type: none"> <li>Assess docs</li> </ul>	<ul style="list-style-type: none"> <li>Outcome report for week's assessments and tests</li> </ul>
	<ul style="list-style-type: none"> <li>Map processes and controls</li> <li>Improvements and gaps analysis</li> <li>Update Framework</li> </ul>	<ul style="list-style-type: none"> <li>Map processes and controls</li> <li>Improvements and gaps analysis</li> <li>Update Framework</li> </ul>	<ul style="list-style-type: none"> <li>Map processes and controls</li> <li>Improvements and gaps analysis</li> <li>Update Framework</li> </ul>	<ul style="list-style-type: none"> <li>Map processes and controls</li> <li>Improvements and gaps analysis</li> <li>Update Framework</li> </ul>	<ul style="list-style-type: none"> <li>Map processes and controls</li> <li>Improvements and gaps analysis</li> <li>Update Framework</li> </ul>
<b>Sabrina</b>	<ul style="list-style-type: none"> <li>run tests</li> <li>look for docs on system</li> </ul>	<ul style="list-style-type: none"> <li>request further docs</li> </ul>			<ul style="list-style-type: none"> <li>manage doc submissions</li> <li>esc list from week</li> </ul>

## Attachment B – Proposed Defence Purchasing and Travel Card Tests

Scenario	Purpose	Tests	Able to be conducted?
Cash advance	To identify suspicious transactions relating to Cash Advance (including Travelex) and to allow these transactions to be followed up.	Transactions >\$950	Yes – Now
		DPC transactions	Yes – Now
		Multiple transactions over consecutive days	Yes – Now
		High volume users	Yes – Now
		Travelex transactions	Yes – Now
Misuse	To identify and follow up suspicious/high risk Credit Card transactions which <u>may</u> be indicative of impropriety	Risky merchants	Currently being done
		Transactions at or after cessation of employment	Yes – Awaiting PMKeys Data
		PayPal transactions	Yes – Now
		Un-acquitted transactions >60days	Currently being done
		Suspicious description (i.e. upgrade, valet, gift, facilitation, personal, massage etc)	No – Analytical tool required (ACL)
		High value transactions >\$10,000	Yes – Now
		High volume users (sample)	Yes – Now
		Duplicate transactions/ Payment splitting (user, vendor, date)	Yes – Now
		DPC transactions outside business hours (weekend/public holiday)	Yes – Now
Travel	To identify and follow up high risk use of taxi services	Transactions undertaken by EA on behalf of SES	No – Additional data required
		Taxi purchases >\$200	Yes – Now
		High volume taxi users	Yes – Now
		High value transactions	Yes – Now

## **Attachment C – Defence Financial Risk Map 2015-16**



[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Thursday, 8 December 2016 14:07  
**To:** Fraud Investigations  
**Cc:** [REDACTED]  
**Subject:** FW: Fraudulent ATM Withdrawal [DLM=Sensitive:Personal]  
**Categories:** No Security Classification Required  
**Attachments:** [REDACTED]  
**Sensitive:** Personal

Good afternoon,

Please find attached information on two ATM cash withdrawals, which have been disputed by the card holder [REDACTED] and confirmed by the bank that the PIN was used.

Note that reimbursement by the bank is not possible when it is identified that the PIN has been used.

The DFAC team have reviewed the attached transactions and noticed several unusual transactions from the card holder, in particular cash withdrawals. These transactions are highlighted in yellow.

I am therefore lead to believe that when it is identified that a disputed transaction has used a PIN that the matter should be referred to your area for further consideration.

If this is not the case please advise otherwise. Otherwise please do not hesitate to contact me if you require any additional reports.

Regards

[REDACTED]  
[REDACTED]  
Defence Financial Assurance and Compliance  
Chief Finance Officer Group  
Department of Defence

R1-2-B027 | PO Box 7909 | Russell Offices)  
CANBERRA ACT 2610  
[REDACTED]

**IMPORTANT:** This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

8/12/2016



**Australian Government**  
**Department of Defence**

Directorate of Financial Assurance and Compliance

## **Group CFO's**

# **Monthly Financial Assurance and Compliance Report –September 2016**

## EXECUTIVE SUMMARY as per SCWRT Report Tabled

19 instances of PGPA non-compliance were recorded for September 2016. They were:

- 18 breaches of PGPA Act s23 (power in relation to arrangements and commitments); and
- 1 breach of PGPA Act s25/26 (duty to act honestly and in good faith).

Miscoding of financial transactions can cause a misrepresentation in financial reporting of certain expense categories and in spend against Group and Service budgets. To the end of September, DFAC's review of ROMAN general ledger account has found a coding error rate of 9.45% or \$11.2m. This miscoding has largely been due to lack of knowledge and understanding of the chart of accounts or negligence. DFAC has identified the main causes of mis-coding and is currently working with the Chart of Accounts team to improve GL code guidance within the Chart of Accounts.

To the end of September 2016, Defence has incurred 117 traffic fines and driving infringements. Reimbursement from the majority cases has been received however, Defence has absorbed a total of \$4,850. Some traffic fines and driving infringements can not be reimbursed due to cultural attitude towards identification of the offending driver. In some instances, traffic fines and administration costs have arisen from driving infringements being charged back to Defence by hire car companies.

## SUMMARY

The Directorate of Financial Assurance and Compliance (DFAC) is tasked with ensuring that Defence and its personnel are complying with Defence Policies, Defence Instructions and Accountable Authority Instructions which are captured under the *Public Governance and Performance Accountability Act 2013* (PGPA Act).

The purpose of this report is to communicate to Groups the types of compliance and assurance issues that are encountered during DFAC's monthly compliance and assurance activities so that Groups can tailor relevant training around these specific issues and or undertake any remediation action as necessary.

During the 2016-17 financial year, the Directorate of Financial Assurance and Compliance (DFAC), will undertake a series of financial assurance and compliance reviews. These reviews assist the CFO in ensuring that Defence's financial information, data and statements are true and accurate. These reviews ensure Defence's compliance with relevant internal and external financial policies, procedures as well as the *Public Governance and Performance Accountability Act 2013* (PGPA Act).

Through out the financial year, DFAC will analyse, identify, report and assist in remediation of financial information and transactions. DFAC will gain assurance over Defence's legislative compliance, as well as to prevent and/or detect fraud and errors, as well as to assist in providing reasonable assurance regarding the reliability of Defence's financial reporting.

During the monthly reviews, DFAC will utilise ROMAN, BORIS, MILIS and ProMASTER, as well as other tools, to:

- assessing operating effectiveness of Defence's financial risk controls;
- monitoring compliance performance for the whole of Defence;
- reducing assurance activity and control testing work duplications;
- ensuring greater accountability for compliance and accurate and true accounting;
- creating consistency across the organisation over timing, nature and extent of assurance and controls testing; and
- creating greater responsibility, accountability and awareness through out Defence.

For the scope of DFAC's planned 2016-17 financial assurance and compliance reviews, please refer to Annex A.



## FINDINGS

Issue and Finding	Comment and Remediation
<b>Late Payments Review</b>	<ul style="list-style-type: none"> <li>• There have been 131 confirmed late payments during the 2016-17 financial year to date. Consequently, Defence must pay \$20,407 interest.</li> <li>• DFAC will organise interest payments to be made by Accounts Payable within Financial Operations to process on behalf of the groups.</li> </ul>
<b>Fines and Infringements Review</b>	<ul style="list-style-type: none"> <li>• During the 2016-17 financial year, Defence has paid 117 traffic fines and driving infringements, totalling \$18,072. Currently Defence has absorbed \$4,850.</li> <li>• Defence is not liable for personal fines and infringements, and any corporate fine or infringement charged to Defence must be re-issued appropriately in the liable personnel's name.</li> </ul>
<b>General Ledger Review</b>	<ul style="list-style-type: none"> <li>• A total of 29,875 transactions were reviewed across 26 ROMAN general ledger accounts during the first quarter of the 2016-17 financial year.</li> <li>• An overall potential error rate of 9.45% has been noted during the first quarter review totalling a potential \$11.2m in miscoding in ROMAN.</li> <li>• DFAC would like to remind CFO staff that all financial data, including the accuracy of GL coding is important to the integrity of Defence's financial reports and information.</li> </ul>
<b>Credit Card High Risk Merchant Review</b>	<ul style="list-style-type: none"> <li>• DFAC has reviewed 327 transactions during the 2016-17 financial year to date.</li> <li>• No intentional mis-usage have been found however, 68 issues have been noted regarding breaches and miscoding.</li> <li>• 56% of requests for confirmation and information were returned to DFAC. DFAC thank ADF and APS staff for the excellent response rate and audit evidence return.</li> </ul>
<b>PGPA Breach Register Review</b> *self-reported on SharePoint	<ul style="list-style-type: none"> <li>• 19 breaches have been self reported on SharePoint during September 2016.</li> <li>• This bring the total instances of non-compliance to 48 for the three months to 30 September 2016-17.</li> <li>• 37 breaches have been reported after July 1 2016 that pertain to breaches in the previous financial year, 2015-16..</li> </ul>

## Review Summaries

During September 2016, DFAC completed a number of reviews of Defence's financial data and information.

Review	Purpose
<b>Late Payments - Confirmation review.</b>	<p>The ROMAN Late Payment report monitors compliance with the Supplier Pay On-Time and or Pay Interest Policy, whereby a payment is not made within the maximum payment terms (30 days), interest accrues to the supplier. This policy applies to contracts valued up to and including \$1 million (GST inclusive) and where interest payable to the supplier is more than \$10 dollars (GST inclusive).</p> <p><b>The purpose of this review is to gain assurance over Defence's financial agreement of payment terms no later than 30 days and in particular to ensure that Defence is not wasting resources on unnecessary interest.</b></p> <p><i>Source: Resource Management Guide No 417 – Supplier Pay On-Time or Pay Interest Policy.</i></p>

DFAC have designed a new, robust review that will investigate to establish whether payments have been made late for the whole of Defence. During this financial review, DFAC will capture how Defence engages with suppliers and will provide assurance over Defence's commitment to suppliers. DFAC's review will reduce the financial risk of poor business processes, resource wastage and budgeting.

DFAC would like to continue to remind financial staff to ensure that all payments and invoices are paid by the due date to avoid interest payments.

## Results – Late Payments Confirmation Review

Month	Payments Reviewed (#)	Payments Reviewed (\$)	Confirmed Late Payments (#)	Confirmed Late Payments (\$)
<b>July-August 2016</b>	420	28.5m	108	<b>17,513</b>
<b>September 2016</b>	748	5.2m	23	<b>2,894</b>
<b>YTD TOTAL 2017</b>	<b>494</b>	<b>33.77m</b>	<b>131</b>	<b>20,407</b>

During the review of late payment transactions and dollar values, DFAC concluded the following:

- It is concerning that Defence will pay late payment interest charges of \$20,503 to the end of September, due to Defence paying contractors, vendors and suppliers late and not as per the terms of the invoice, contract or agreement. This is not considered efficient, effective or economical use of public funds and Defence's resources.
- The response rate from the groups regarding confirmations and audit evidence requests is approximately 72%. It is imperative that all requests for confirmations or documentation is met in a timely manner as per the request. Where the payment is not made within the maximum payment terms, Defence is to pay interest to the supplier. Failure to pay the interest to the relevant supplier will be considered as a breach against the RMG 417 Supplier Pay On Time or Pay Interest Policy
- If you have outstanding requests for information or confirmation, please respond immediately.
- As per the Defence Group information below, as of September 2016, the CASG has the highest rate of late payments confirmed at 73.

Group	Confirmed Late Payments YTD (#)	Confirmed Late Payments Interest Owing YTD (\$)	Response Rate (%) YTD
<b>Air Force</b>	3	344.83	60
<b>Army</b>	3	97.88	100
<b>Associate Secretary</b>	11	781.01	49
<b>CASG</b>	73	13,996.21	81
<b>CFO</b>	0	0	N/A
<b>DSTG</b>	22	3635.49	100
<b>JOC</b>	0	0	100
<b>Navy</b>	6	124.10	100
<b>SP&amp;I</b>	1	16.77	18
<b>VCDF</b>	14	928.9	55
<b>TOTAL YTD 2017</b>	<b>133</b>	<b>19,925.19</b>	<b>72</b>

Review	Purpose
Late Payments - Compliance Review	<p>The purpose of this review is to analyse and review a sample selection of confirmed late interest payments. This is to ensure correct and appropriate procedures and policies have been implemented and appropriately followed when a payment is late. This also included the correct calculation of interest owing.</p> <p><i>Source: Resource Management Guide (RMG) 417 – Supplier Pay On Time or Pay Interest Policy</i></p>

As with Confirmation reviews with late payments, DFAC will also be implementing a Defence wide, robust new testing program during September 2016. There are currently no breaches to report as groups have until October 6 2016 to respond regarding late payments and possible breaches. Results for the first quarter will be reported in the November DFAC Assurance and Compliance Monthly Report.

Review	Purpose
<b>Fines and Infringements Review</b>	<p>The purpose of this review is to analyse and review any traffic fines or driving infringements that Defence has incurred on behalf of APS, ADF or Defence guests. This is to ensure correct and appropriate procedures and policies have been implemented and appropriately followed if Defence has incurred a fine or infringement payment is late. This monthly review reduces the financial risk of credit card mis-use and the mis-use of public monies.</p> <p><i>Any APS, ADF or other liable personnel who has incurred a traffic fine or driving infringement should not allow to be paid by Defence in the first instance. Rather the corporate fine should be re-issued in the appropriate liable personnel's name as a civilian fine. If any costs have been incurred to Defence such as administration fees from hire companies, the liable personnel will be required to repay any monies paid by Defence on their behalf.</i></p>

### **Results – Fines and Infringements Review**

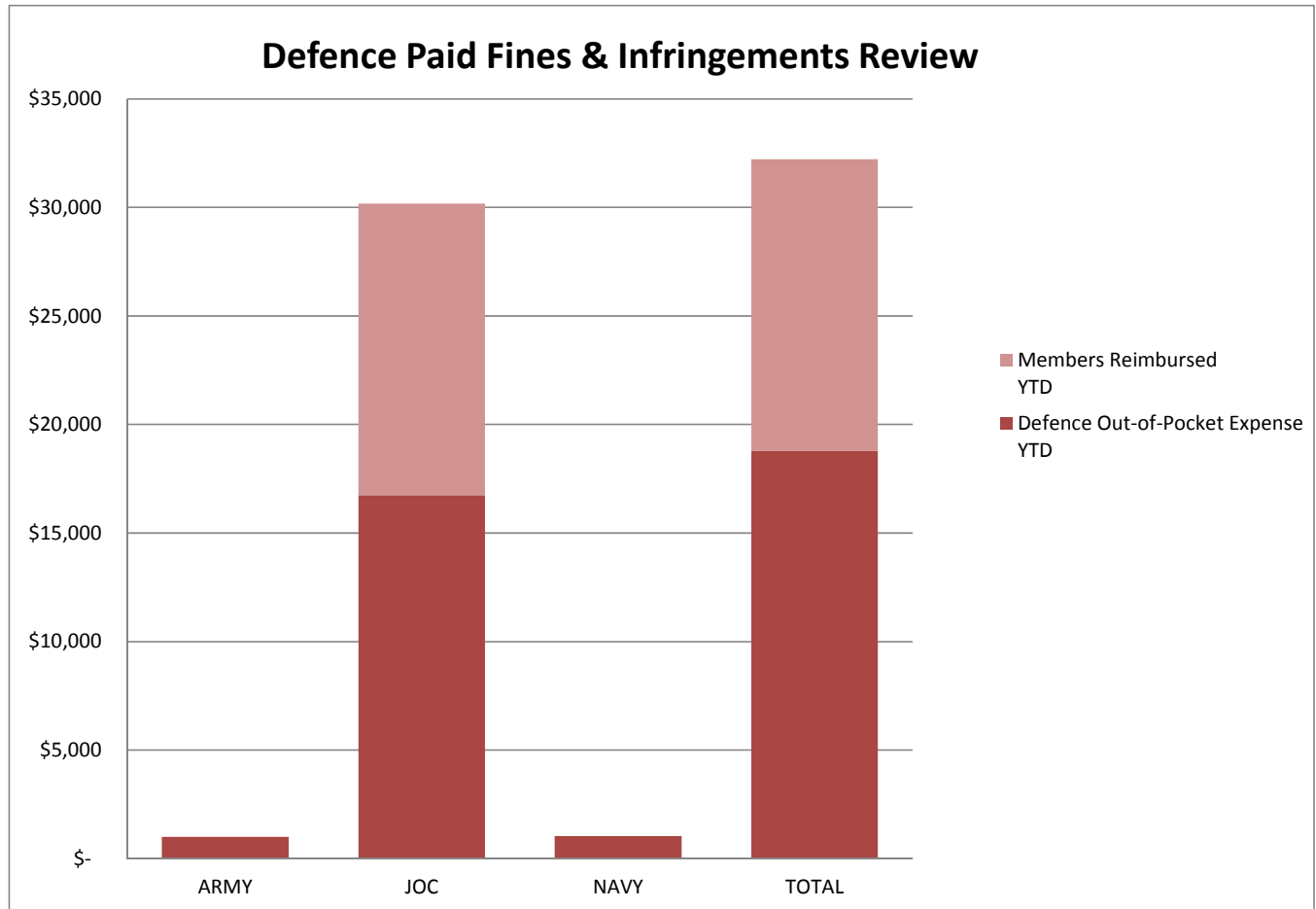
To the end of September 2016, 117 traffic fines and driving infringements have been paid by the Department of Defence. Of these 117 Defence paid fines, only 90 have been reimbursed by the relevant members and drivers. This has left Defence out-of-pocket over \$4,850.

Month	Defence Paid Transaction (#)	Defence Paid (\$)	Members Reimbursed (\$)	Defence Out-of-Pocket (\$)
<b>July – August 2016</b>	71	10,200	9,495	<b>705</b>
<b>September 2016</b>	46	7,872	3,640	<b>4,145</b>
<b>YTD TOTAL 2017</b>	<b>117</b>	<b>18,072</b>	<b>13,135</b>	<b>4,850</b>

Group	Fines and Infringements September (#)	Fines and Infringements paid YTD 2016-17 (#)	Fines and Infringements paid YTD 2016-17 (\$)
<b>ARMY</b>	2	2	1,006
<b>ARMY – JOC</b>	42	115	17,066
<b>TOTAL</b>	<b>44</b>	<b>117</b>	<b>18,072</b>

As per the above table, the majority of traffic fines that have been paid by Defence this financial year relate to traffic fines incurred by ARMY JOC members in the UAE. JOC has a process of raising account receivables and requesting reimbursement directly from the drivers identified by the unit. This is due to the inability of the unit to identify the driver directly to the UAE Dubai Police General H.Q. General Department of Finance. DFAC has noted that these fines and infringements have been incorrectly posted to ROMAN General Ledger Code 21022 Hire and Other Fees.

Army has paid an historic fine during September, from a fine incurred in May 2012. Due to the lack of action in a timely manner, Defence has so far been unable to locate the responsible driver or member. This fine has not been reimbursed and no member held accountable.



Review	Purpose
<b>Forensic General Ledger Coding Review</b>	<p>The purpose of this review is to provide a level of assurance that Defence's financial information is accurate, that transactions are correctly attributed to either assets liabilities, expense or revenue and expenditure is recorded in the correct GL account. This review provides assurance over the expense groups in ROMAN.</p> <p>To achieve this purpose DFAC analyse ROMAN transactions for selected GL codes with the aim of identity miss-coded transactions. Defence reviewed 26 ROMAN GL codes during the first quarter to 30 September 2016. The results are summarised in the table below.</p> <p>Source: General Ledger Account Codes - <a href="http://intranet.defence.gov.au/find/chart_of_accounts/GLAccountCodes.asp">http://intranet.defence.gov.au/find/chart_of_accounts/GLAccountCodes.asp</a></p>

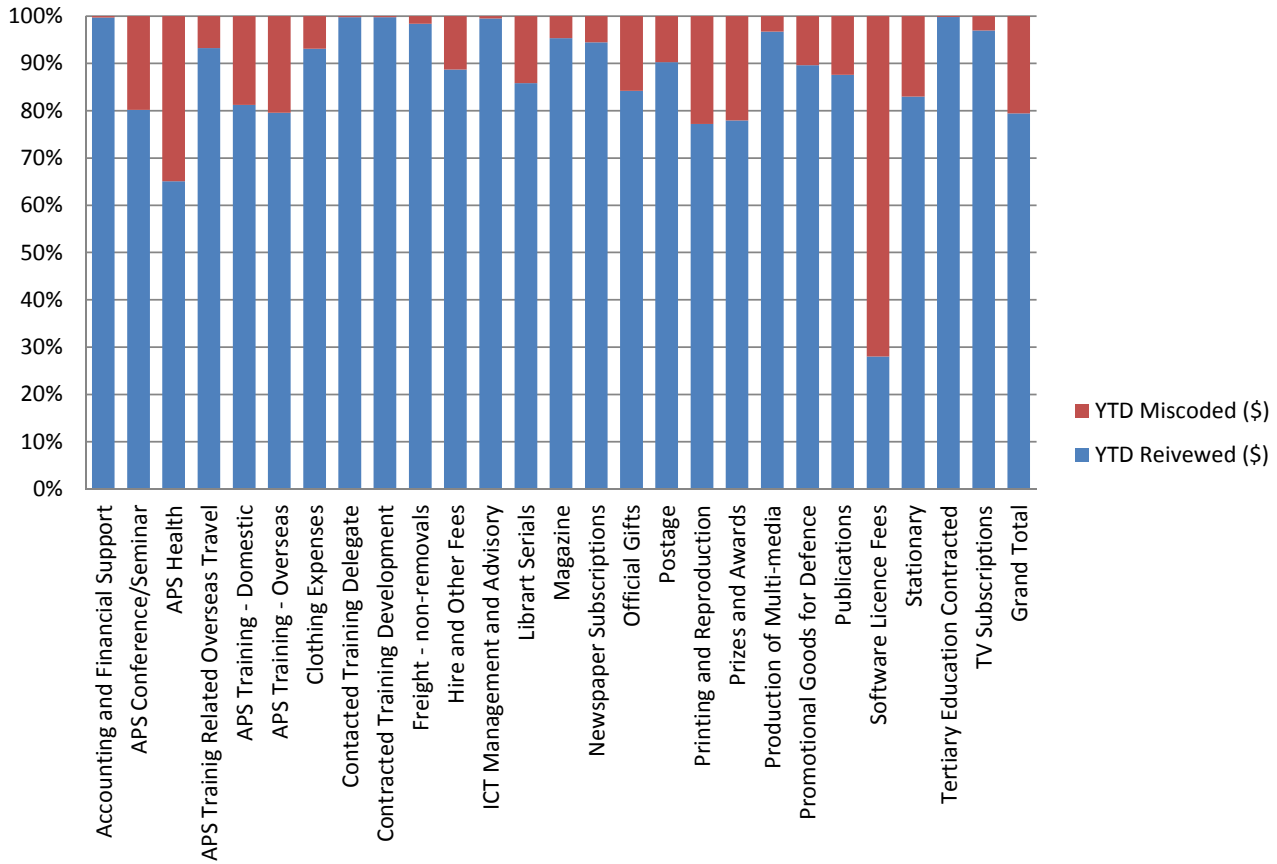
### **Results – Forensic General Ledger Coding Review**

Month	Review Size Transactions (#)	Review Size Dollar Value (\$)	Miscoded Transactions (#)	Miscoded Dollar Value (\$)	Ratio of Miscoding (%)
<b>July – August 2016</b>	18,924	65.99m	2,766	4.7m	<b>16.24</b>
<b>September 2016</b>	10,951	52.9m	1,284	6.5m	<b>12.20</b>
<b>YTD TOTAL 2017</b>	<b>29,875</b>	<b>118.9m</b>	<b>4,050</b>	<b>11.2m</b>	<b>9.45</b>

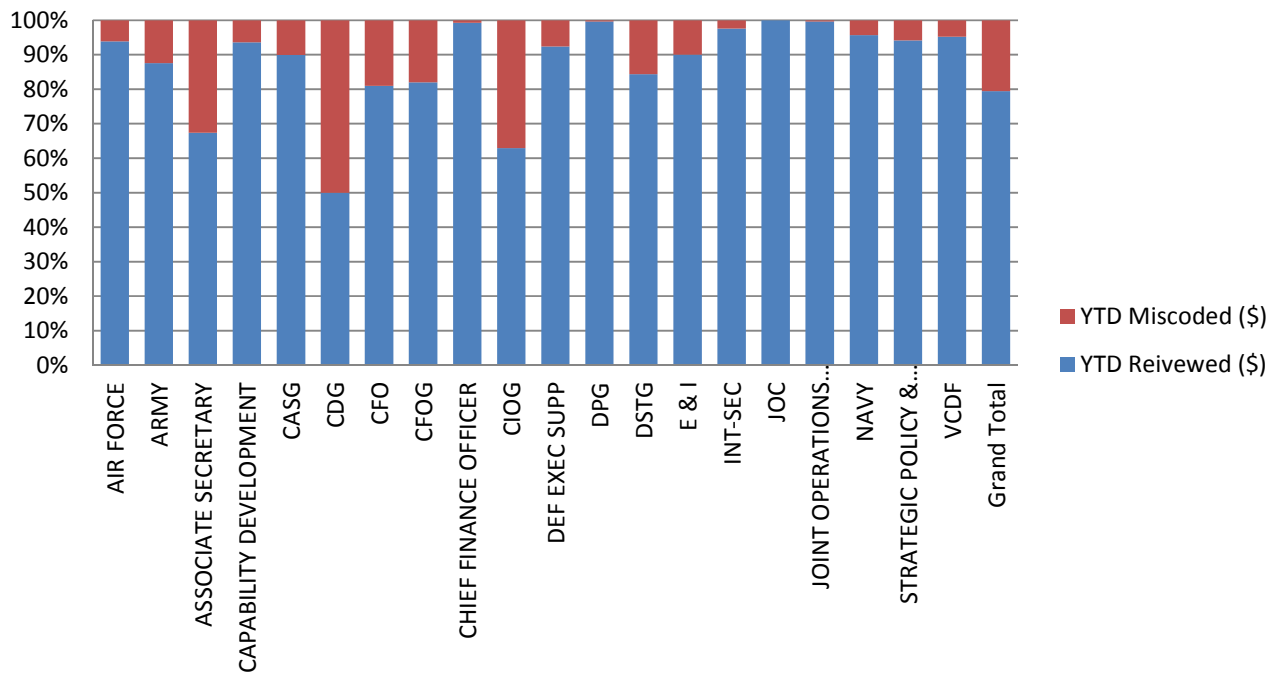
During the review of Defence's ROMAN GL Codes, DFAC concluded the following:

- DFAC reviewed a total of 26 ROMAN GL codes during Quarter 1.
- An unacceptably high error rate of 12.20% was noted for September 2016, bringing the year to date percentage of error by quantity to 9.45%. Incorrect coding can lead to inaccurate reporting, incorrect budgeting and increase the risk of financial misstatement.
- This level of error highlights possible need for re-education amongst Defence member's who enter financial information into Defence's financial systems. It also highlights the need for a review of Defence's GL coding and classifications provided on the FiND website. Many areas have requested more clear and concise guidance and explanations on the FiND website. DFAC is meeting with the Chart of Account team to explore and implement avenues to improve current guidance.
- It is vitally important that Defence has the highest level of confidence in its financial systems and the data within. Supervisors must ensure that expenditure is transacted appropriately, and that all staff inputting data in to ROMAN have sufficient training and available resources. If members are unsure as to how to attribute costs or the GL Look Up on the FiND website, please contact the GL Code mailbox or DFAC staff for assistance.

## ROMAN General Ledger Miscoding Review



## ROMAN General Ledger Miscoding Review





Review	Purpose
<b>Credit Card – High Risk Merchant Review</b>	<p>The purpose of this review is to analyse and review a sample selection of credit card transactions that have been attributed to “High Risk” merchant categories. These merchant categories are set at PoS (Point-of-Sale) by the banks, and Defence review 53 categories including antiques stores, jewellery shops and cigar stands. Defence reviews a sample of transactions in these high risk categories to ensure compliance with Defence expenditure, and to ensure appropriate use of Defence resources.</p> <p><b>DFAC ensures that Defence’s expenditure is appropriate, approved and efficient and effective use of public money. This review minimises the financial risk of credit card fraud or mis-use.</b></p> <p><i>Source: Accountable Authority Instructions Chapter 5. and Defence Procurement Policy Manual Para 53-59 and 63-70.</i></p>

### Results – Credit Card High Risk Merchant Review

Month	Transactions Sampled (#)	Reviewed Transactions (\$)	Transactions Reviewed (#)	Transactions Reviewed (\$)
<b>July – August 2016</b>	131	228,551	82	130,058
<b>September 2016</b>	196	582,350	53	150,643
<b>YTD TOTAL 2017</b>	<b>327</b>	<b>810,900</b>	<b>0</b>	<b>280,701</b>

Month	To be Reviewed (#)	To be Reviewed (\$)	NIL Response (#)	Response Rate (%)
<b>July – August 2016</b>	0	0	49	59.76
<b>September 2016</b>	47	150,721	96	52.00
<b>YTD TOTAL 2017</b>	<b>47</b>	<b>150,721</b>	<b>145</b>	<b>55.66</b>

During the review of Defence's Credit Card High Risk Merchant Review, DFAC noted the following:

- Although DFAC found no intentional mis-use regarding Defence expenditure, DFAC found several concerning issues such as:
  - failure to obtain appropriate delegate approvals;
  - record keeping;
  - using incorrect general ledger; and
  - ignoring expenditure justification.
- As part of expenditure of funds, Defence members must provide sufficient justification. DFAC has noticed members have not completed the justification for expenditure or have wrote very generic responses, for example "The shop was close". Members must at all times be able to justify the expenditure of public monies in efficient, effective, ethical and economical way.

<b>Group</b>	<b>Number of Transactions Miscoded (#)</b>	<b>Number of Transactions Miscoded (\$)</b>	<b>Potential Breach (#)</b>	<b>PGPA Breaches Yet to be Reported (\$)</b>
<b>Air Force</b>	7	3,480	5	1,940
<b>Army</b>	15	101,795	13	7,810
<b>CASG</b>	1	6,275	0	0
<b>CIOG</b>	2	2,589	3	8,167
<b>DPG</b>	0	0	2	11,362
<b>DSTG</b>	1	26	1	1,1562
<b>E&amp;I</b>	0	0	1	6,899
<b>JOC</b>	1	4,590	4	9,547
<b>NAVY</b>	5	2,398	3	3,895
<b>SP&amp;I</b>	0	0	1	-66
<b>VCDF</b>	0	0	3	28,626
<b>YTD TOTAL 2017</b>	<b>32</b>	<b>30,155</b>	<b>36</b>	<b>\$79,745</b>

- It has been noted that some members of the ADF once posted or relocated, no longer have access or copies of supportive documentation and/or documentation has not been appropriately filed. It is the card holder responsibility to locate their own documentation including requesting the documentation from the former unit.
- Some card holders are unaware of the procedures to follow for disputed transactions. Supportive documentation has not been appropriately filed. Documentation regarding fraudulent or incorrect charges must be kept and/or filed.
- Always report unusual or unexpected credit card transactions immediately or in a timely manner. DFAC have reviewed a transaction in which the card holder noticed unexpected transactions (a result of illegal card skimming), however did not complete the appropriate procedure and the card was skimmed multiple times over multiple months prior to any action being taken, including the cancellation of the skimmed card.

Review	Purpose
<b>Compliance Report Testing</b>	<p>Section 19 of the PGPA Act 2013 requires that Defence notify the Minister of all significant non-compliance against the PGPA Act 2013.</p> <p>Non-compliance data is captured through the SharePoint Compliance Reporting Portal. The purpose of this review is to analyse this data, determine the nature of the non-compliance and report on results.</p> <p>The particular focus is on identifying and analysing significant non-compliance.</p> <p>Source: <a href="http://intranet.defence.gov.au/find/policies/compliance_reporting.html">http://intranet.defence.gov.au/find/policies/compliance_reporting.html</a></p>

### Results – Compliance Report Review

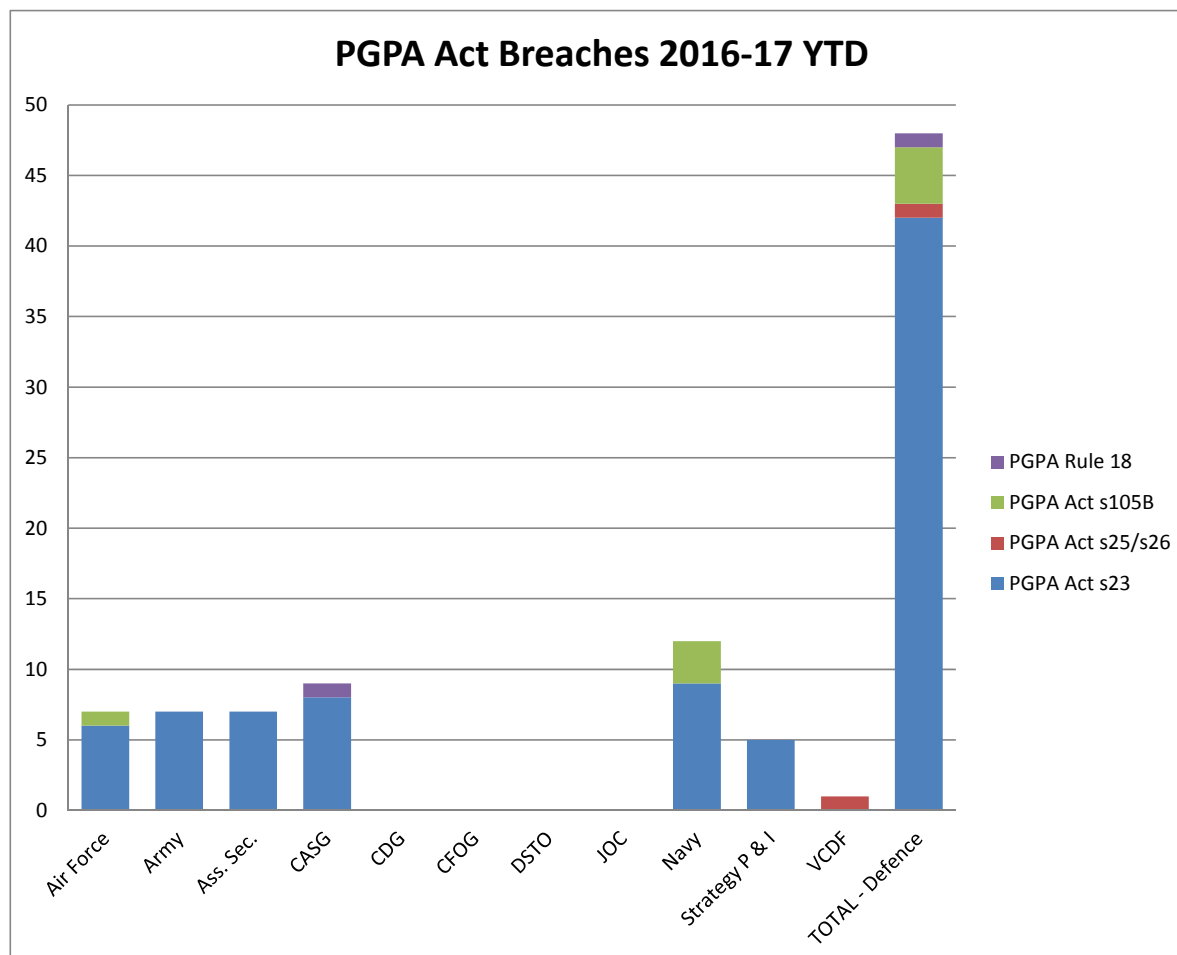
PGPA Breach	Non-Compliance September 2016	Non-Compliance YTD 2016-17
<b>PGPA s23 – Power in relation to arrangements and commitments</b>	18	42
<b>PGPA s25/S26 – Duty of care and due diligence, Duty to act honestly, in good faith and for a proper purpose</b>	1	1
<b>PGPA s105B – Instruments relating to procurement</b>	0	4
<b>PGPA Rule 18 – Approving commitments of relevant money</b>	0	1
<b>Officials PGPA Rule 9</b>	0	0
<b>Total PGPA Non-Compliance - Self Reported*</b>	<b>19</b>	<b>48</b>

\*As per SharePoint Compliance Register (self-reporting).

Please note for detail of Group non-compliance, please view the applicable Group folder in DFAC's *External Parties Folder* in Objective.

Group	PGPA Act s23	PGPA Act s25/26	PGPA Act S105B	PGPA Act Rule 18	Total YTD 2016-17
Air Force	6	0	1	0	7
Army	7	0	0	0	7
Associate Secretary	7	0	0	0	7
CASG	8	0	0	1	9
CDG	0	0	0	0	0
CFOG	0	0	0	0	0
DSTO	0	0	0	0	0
JOC - Army	0	0	0	0	0
Navy	9	0	3	0	12
Strategy Policy	5	0	0	0	5
VCDF	0	1	0	0	1
<b>Total PGPA Breaches</b>	<b>42</b>	<b>1</b>	<b>4</b>	<b>1</b>	<b>48</b>

\*As per SharePoint Compliance Register (self-reporting).



### **Summary of Non-compliance**

- Non –compliance against the PGPA Act totalled 19 reportable instances for September 2016.
- 48 instances of non-compliance have been self-reported during the 2016-17 financial year. 42 instances were reported as non-compliance with s23 of the PGPA Act. These instances occurred as a result of:
  - failures to obtain appropriate delegate approvals prior to entering into or varying an agreement;
  - exceeding delegate approval; and
  - non-compliance related to travel arrangements.
- The four instances of non-compliance reported against PGPA Section 105B, which relates to the failure to use Whole of Government Procurement Guidelines when required.
- The one instance of non-compliance against Section 26 occurred when a Defence official used a Defence Purchase Card for personal purposes. The amount involved was \$15.95, that has since been repaid to Defence..

It is noted that corrective action has been taken against all instances of non-compliance. This mainly involved counselling of staff and providing additional training.

Defence staff have reported a further 37 instances of non-compliance pertaining to the previous financial 2015-16 during the first quarter 2016-17. These instances are not reportable for end of year Compliance Reporting Purposes.

Review	Purpose
<b>CMS Data Review</b>	<p><b>The purpose of this review is to analyse, review and report Defence's use of the corporate card system including expenditure trends.</b></p> <p>DFAC ensures that Defence's financial data is true and accurate.</p> <p>DFAC have developed a testing program designed to improve the forensic/business data analysis work being undertaken by DFAC. DFAC are currently testing expenditure related to taxi usage and cash advances/withdrawals. Assurance and compliance of transactions will commence once streamlined processes for data testing are implemented.</p> <p><i>Source: Accountable Authority Instructions Ch 5. and Defence Procurement Policy Manual Para 53-59 and 63-70.</i></p>

Review	Purpose
<b>Segregation of Duty</b>	<p><b>The purpose of this review is to analyse, review and report Defence's use of the corporate card system including expenditure trends.</b></p> <p>This is to enhance the Financial Controls Framework and Control Testing and ensure Defence's compliance with AASB101.</p> <p>DFAC have reviewed current Segregation of Duty matrix used by CIOG for management of ROMAN user access in order to replace generic risk description with specific description</p> <p>This task ensure that Defence identify and mitigate controls and risk of financial misstatement. Provide advice and ongoing implementation.</p>

- DFAC have reviewed 34 of the 76 Segregation of Duties roles, with 33 roles forwarded to CIOG for comment and advice.
- 28 Risk IDs have been completed. 750 Risk IDs will continue to be reviewed by DFAC.
- With consultation with CFOG-DFO, DFAC have prepared for implementation a semi-annual Defence enterprise wide credit card fraud risk assessment report.
- DFAC have consolidated 11 semi-annual Fraud Risk Assessment reports from 51 Directorates for CFOG. DFAC will review the remaining 5 Fraud Risk Assessment reports. The consolidation process ensures a more efficient and timely reporting during the round as a result of receiving returns from branch heads rather than individual directorates.

Review	Purpose
Gifts, hospitality and sponsorship (GHS)	<p><b>In the past detail of GHS items have been required to respond to Questions on Notice and Senate Estimates briefings. In order to quickly and effectively respond, DFAC established the GHS SharePoint register.</b></p> <p>DFAC staff ensure the completeness and accuracy in GHS reporting by examining all SharePoint entries and conducting completeness reviews.</p> <p>DFAC also run the GHS mailbox, answer ongoing queries and concerns, as well as provides access to the Objective External GHS Folders.</p>

- DFAC answered 8 policy related questions during September.
- DFAC was required to amend 2 separate reported GHS transactions.
- DFAC provided 2 member access to the Objective External GHS Folders.
- DFAC responded to 2 general enquiries regarding GHS.

If you have any enquiries, please email the DFAC's group mailbox at CFO FBI FAC, [cfofbifac@defence.gov.au](mailto:cfofbifac@defence.gov.au). We will respond to enquiry within 2 business days. For specific enquires please see the point of contacts below.

- Late Payments, Defence Credit Cards High Risk Merchant Categories, Invoice Overview, Fines and Infringements, CFOG DREAMS Tokens, CMS potential miscoding: Sandra Cole on (02) 626 54835, [sandra.cole@defence.gov.au](mailto:sandra.cole@defence.gov.au).
- General Ledger Forensic Data Analysis and PGPA Compliance Overview: Michael Sharp (02) 626 5 7455, [michael.sharp4@defence.gov.au](mailto:michael.sharp4@defence.gov.au).

Susan McLean

A/Director Financial Assurance and Compliance

September 2016



## ANNEX A

### DFAC 2016- 17 Scope and plan for works

DFAC will undertake monthly, quarterly, ad-hoc and yearly reviews in the following areas. DFAC may undertake more or less testing based on Defence's assurance and compliance needs.

Review	Proposed Timing	Purpose
<b>Compliance Report Testing</b>	On-going, monthly	To ensure that Defence complies with the PGPA Act
<b>Gifts, Hospitality and Sponsorship (GHS)</b>	On-going, monthly	To ensure Defence correctly registers and reports GHS, as well as answer QoNs and Senate Estimates.
<b>Forensic GL Reviews</b>	On-going, monthly	To ensure that Defence's financial information is correct and accurate, that all assets are classified correctly and expenditure is appropriate.
<b>Late Payment Review</b>	On-going, monthly	To ensure that Defence meets its financial obligation and to reduce the level of resource wastage and expenditure.  To report on transactions and dollar value of late payments, as well as compliance with processes and procedures.
<b>Reason Code Review</b>	On-going, monthly	To ensure that Defence's financial information is to true and accurate and reflects appropriately.
<b>Credit Card – High Risk Merchant Review</b>	On-going, monthly	To ensure that Defence's expenditure is appropriate, approved and efficient and effective use of public money. This review minimises the financial risk of credit card fraud or mis-use.
<b>Forensic Business Review</b>	Ongoing, monthly	This is to enhance the Financial Controls Framework and Control Testing and ensure Defence's compliance with AASB101.
<b>Defence Financial Controls Framework</b>	Ongoing	This task ensure that Defence identify and mitigate controls and risk of financial misstatement. Provide advice and ongoing implementation.
<b>Fines and Infringements Review</b>	Ongoing, monthly	This task is to ensure that Defence does not incur any fines or infringements on behalf of its members. The review reduces the financial risk of credit card mis-use and the mis-use of public monies.



**Australian Government**  
**Department of Defence**

Directorate of Financial Assurance and Compliance

## **Group CFO's**

# **Monthly Financial Assurance and Compliance Report –September 2016**

## EXECUTIVE SUMMARY as per SCWRT Report Tabled

19 instances of PGPA non-compliance were recorded for September 2016. They were:

- 18 breaches of PGPA Act s23 (power in relation to arrangements and commitments); and
- 1 breach of PGPA Act s25/26 (duty to act honestly and in good faith).

Miscoding of financial transactions can cause a misrepresentation in financial reporting of certain expense categories and in spend against Group and Service budgets. To the end of September, DFAC's review of ROMAN general ledger account has found a coding error rate of 9.45% or \$11.2m. This miscoding has largely been due to lack of knowledge and understanding of the chart of accounts or negligence. DFAC has identified the main causes of mis-coding and is currently working with the Chart of Accounts team to improve GL code guidance within the Chart of Accounts.

To the end of September 2016, Defence has incurred 117 traffic fines and driving infringements. Reimbursement from the majority cases has been received however, Defence has absorbed a total of \$4,850. Some traffic fines and driving infringements can not be reimbursed due to cultural attitude towards identification of the offending driver. In some instances, traffic fines and administration costs have arisen from driving infringements being charged back to Defence by hire car companies.

## SUMMARY

The Directorate of Financial Assurance and Compliance (DFAC) is tasked with ensuring that Defence and its personnel are complying with Defence Policies, Defence Instructions and Accountable Authority Instructions which are captured under the *Public Governance and Performance Accountability Act 2013* (PGPA Act).

The purpose of this report is to communicate to Groups the types of compliance and assurance issues that are encountered during DFAC's monthly compliance and assurance activities so that Groups can tailor relevant training around these specific issues and or undertake any remediation action as necessary.

During the 2016-17 financial year, the Directorate of Financial Assurance and Compliance (DFAC), will undertake a series of financial assurance and compliance reviews. These reviews assist the CFO in ensuring that Defence's financial information, data and statements are true and accurate. These reviews ensure Defence's compliance with relevant internal and external financial policies, procedures as well as the *Public Governance and Performance Accountability Act 2013* (PGPA Act).

Through out the financial year, DFAC will analyse, identify, report and assist in remediation of financial information and transactions. DFAC will gain assurance over Defence's legislative compliance, as well as to prevent and/or detect fraud and errors, as well as to assist in providing reasonable assurance regarding the reliability of Defence's financial reporting.

During the monthly reviews, DFAC will utilise ROMAN, BORIS, MILIS and ProMASTER, as well as other tools, to:

- assessing operating effectiveness of Defence's financial risk controls;
- monitoring compliance performance for the whole of Defence;
- reducing assurance activity and control testing work duplications;
- ensuring greater accountability for compliance and accurate and true accounting;
- creating consistency across the organisation over timing, nature and extent of assurance and controls testing; and
- creating greater responsibility, accountability and awareness through out Defence.

For the scope of DFAC's planned 2016-17 financial assurance and compliance reviews, please refer to Annex A.

## FINDINGS

Issue and Finding	Comment and Remediation
<b>Late Payments Review</b>	<ul style="list-style-type: none"> <li>• There have been 131 confirmed late payments during the 2016-17 financial year to date. Consequently, Defence must pay \$20,407 interest.</li> <li>• DFAC will organise interest payments to be made by Accounts Payable within Financial Operations to process on behalf of the groups.</li> </ul>
<b>Fines and Infringements Review</b>	<ul style="list-style-type: none"> <li>• During the 2016-17 financial year, Defence has paid 117 traffic fines and driving infringements, totalling \$18,072. Currently Defence has absorbed \$4,850.</li> <li>• Defence is not liable for personal fines and infringements, and any corporate fine or infringement charged to Defence must be re-issued appropriately in the liable personnel's name.</li> </ul>
<b>General Ledger Review</b>	<ul style="list-style-type: none"> <li>• A total of 29,875 transactions were reviewed across 26 ROMAN general ledger accounts during the first quarter of the 2016-17 financial year.</li> <li>• An overall potential error rate of 9.45% has been noted during the first quarter review totalling a potential \$11.2m in miscoding in ROMAN.</li> <li>• DFAC would like to remind CFO staff that all financial data, including the accuracy of GL coding is important to the integrity of Defence's financial reports and information.</li> </ul>
<b>Credit Card High Risk Merchant Review</b>	<ul style="list-style-type: none"> <li>• DFAC has reviewed 327 transactions during the 2016-17 financial year to date.</li> <li>• No intentional mis-usage have been found however, 68 issues have been noted regarding breaches and miscoding.</li> <li>• 56% of requests for confirmation and information were returned to DFAC. DFAC thank ADF and APS staff for the excellent response rate and audit evidence return.</li> </ul>
<b>PGPA Breach Register Review</b> *self-reported on SharePoint	<ul style="list-style-type: none"> <li>• 19 breaches have been self reported on SharePoint during September 2016.</li> <li>• This bring the total instances of non-compliance to 48 for the three months to 30 September 2016-17.</li> <li>• 37 breaches have been reported after July 1 2016 that pertain to breaches in the previous financial year, 2015-16..</li> </ul>

## Review Summaries

During September 2016, DFAC completed a number of reviews of Defence's financial data and information.

Review	Purpose
<b>Late Payments - Confirmation review.</b>	<p>The ROMAN Late Payment report monitors compliance with the Supplier Pay On-Time and or Pay Interest Policy, whereby a payment is not made within the maximum payment terms (30 days), interest accrues to the supplier. This policy applies to contracts valued up to and including \$1 million (GST inclusive) and where interest payable to the supplier is more than \$10 dollars (GST inclusive).</p> <p><b>The purpose of this review is to gain assurance over Defence's financial agreement of payment terms no later than 30 days and in particular to ensure that Defence is not wasting resources on unnecessary interest.</b></p> <p><i>Source: Resource Management Guide No 417 – Supplier Pay On-Time or Pay Interest Policy.</i></p>

DFAC have designed a new, robust review that will investigate to establish whether payments have been made late for the whole of Defence. During this financial review, DFAC will capture how Defence engages with suppliers and will provide assurance over Defence's commitment to suppliers. DFAC's review will reduce the financial risk of poor business processes, resource wastage and budgeting.

DFAC would like to continue to remind financial staff to ensure that all payments and invoices are paid by the due date to avoid interest payments.

## Results – Late Payments Confirmation Review

Month	Payments Reviewed (#)	Payments Reviewed (\$)	Confirmed Late Payments (#)	Confirmed Late Payments (\$)
<b>July-August 2016</b>	420	28.5m	108	<b>17,513</b>
<b>September 2016</b>	748	5.2m	23	<b>2,894</b>
<b>YTD TOTAL 2017</b>	<b>494</b>	<b>33.77m</b>	<b>131</b>	<b>20,407</b>

During the review of late payment transactions and dollar values, DFAC concluded the following:

- It is concerning that Defence will pay late payment interest charges of \$20,503 to the end of September, due to Defence paying contractors, vendors and suppliers late and not as per the terms of the invoice, contract or agreement. This is not considered efficient, effective or economical use of public funds and Defence's resources.
- The response rate from the groups regarding confirmations and audit evidence requests is approximately 72%. It is imperative that all requests for confirmations or documentation is met in a timely manner as per the request. Where the payment is not made within the maximum payment terms, Defence is to pay interest to the supplier. Failure to pay the interest to the relevant supplier will be considered as a breach against the RMG 417 Supplier Pay On Time or Pay Interest Policy
- If you have outstanding requests for information or confirmation, please respond immediately.
- As per the Defence Group information below, as of September 2016, the CASG has the highest rate of late payments confirmed at 73.

Group	Confirmed Late Payments YTD (#)	Confirmed Late Payments Interest Owing YTD (\$)	Response Rate (%) YTD
<b>Air Force</b>	3	344.83	60
<b>Army</b>	3	97.88	100
<b>Associate Secretary</b>	11	781.01	49
<b>CASG</b>	73	13,996.21	81
<b>CFO</b>	0	0	N/A
<b>DSTG</b>	22	3635.49	100
<b>JOC</b>	0	0	100
<b>Navy</b>	6	124.10	100
<b>SP&amp;I</b>	1	16.77	18
<b>VCDF</b>	14	928.9	55
<b>TOTAL YTD 2017</b>	<b>133</b>	<b>19,925.19</b>	<b>72</b>

Review	Purpose
Late Payments - Compliance Review	<p>The purpose of this review is to analyse and review a sample selection of confirmed late interest payments. This is to ensure correct and appropriate procedures and policies have been implemented and appropriately followed when a payment is late. This also included the correct calculation of interest owing.</p> <p><i>Source: Resource Management Guide (RMG) 417 – Supplier Pay On Time or Pay Interest Policy</i></p>

As with Confirmation reviews with late payments, DFAC will also be implementing a Defence wide, robust new testing program during September 2016. There are currently no breaches to report as groups have until October 6 2016 to respond regarding late payments and possible breaches. Results for the first quarter will be reported in the November DFAC Assurance and Compliance Monthly Report.

Review	Purpose
<b>Fines and Infringements Review</b>	<p>The purpose of this review is to analyse and review any traffic fines or driving infringements that Defence has incurred on behalf of APS, ADF or Defence guests. This is to ensure correct and appropriate procedures and policies have been implemented and appropriately followed if Defence has incurred a fine or infringement payment is late. This monthly review reduces the financial risk of credit card mis-use and the mis-use of public monies.</p> <p><i>Any APS, ADF or other liable personnel who has incurred a traffic fine or driving infringement should not allow to be paid by Defence in the first instance. Rather the corporate fine should be re-issued in the appropriate liable personnel's name as a civilian fine. If any costs have been incurred to Defence such as administration fees from hire companies, the liable personnel will be required to repay any monies paid by Defence on their behalf.</i></p>

### **Results – Fines and Infringements Review**

To the end of September 2016, 117 traffic fines and driving infringements have been paid by the Department of Defence. Of these 117 Defence paid fines, only 90 have been reimbursed by the relevant members and drivers. This has left Defence out-of-pocket over \$4,850.

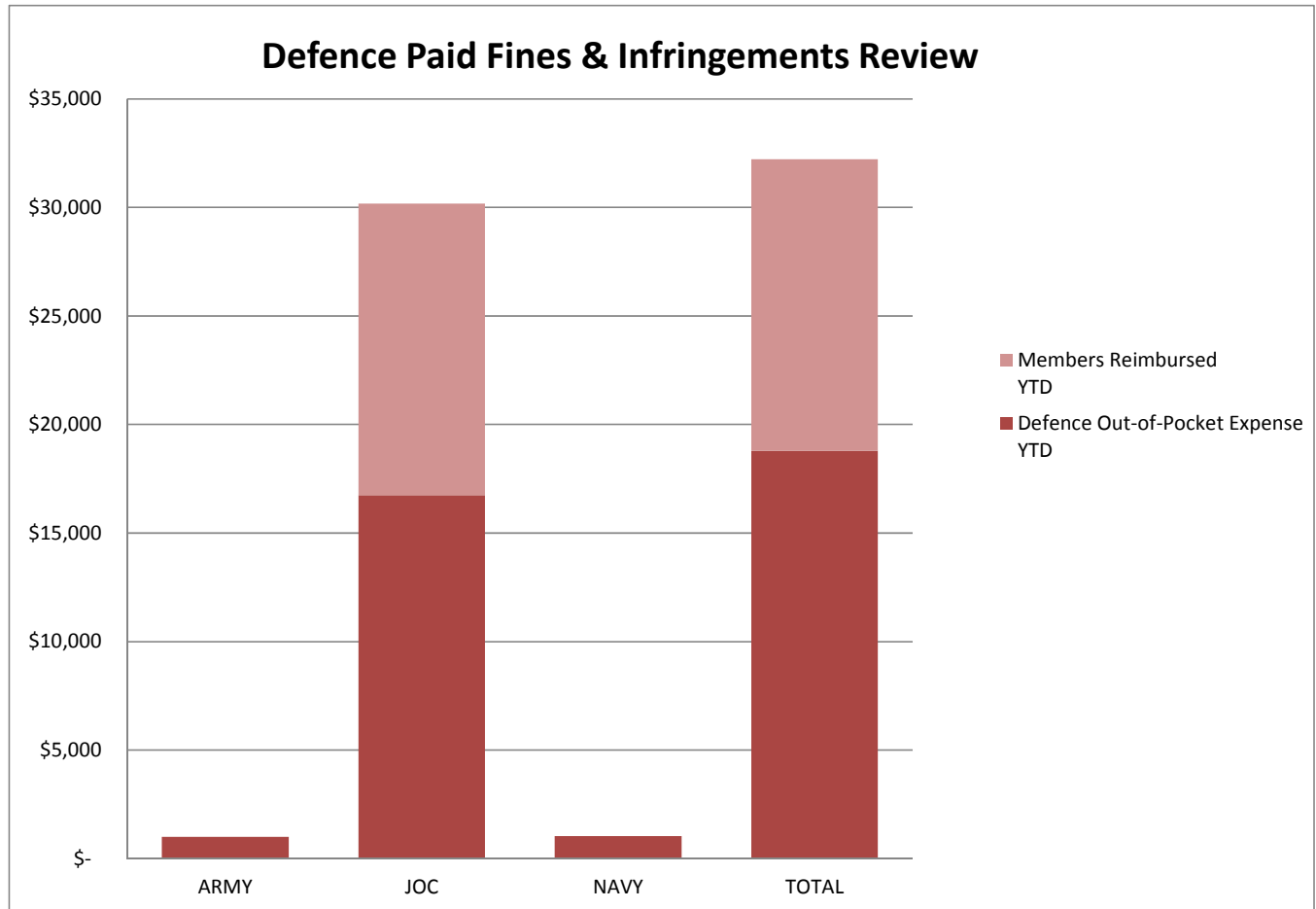
Month	Defence Paid Transaction (#)	Defence Paid (\$)	Members Reimbursed (\$)	Defence Out-of-Pocket (\$)
<b>July – August 2016</b>	71	10,200	9,495	<b>705</b>
<b>September 2016</b>	46	7,872	3,640	<b>4,145</b>
<b>YTD TOTAL 2017</b>	<b>117</b>	<b>18,072</b>	<b>13,135</b>	<b>4,850</b>

Group	Fines and Infringements September (#)	Fines and Infringements paid YTD 2016-17 (#)	Fines and Infringements paid YTD 2016-17 (\$)
<b>ARMY</b>	2	2	1,006
<b>ARMY – JOC</b>	42	115	17,066
<b>TOTAL</b>	<b>44</b>	<b>117</b>	<b>18,072</b>



As per the above table, the majority of traffic fines that have been paid by Defence this financial year relate to traffic fines incurred by ARMY JOC members in the UAE. JOC has a process of raising account receivables and requesting reimbursement directly from the drivers identified by the unit. This is due to the inability of the unit to identify the driver directly to the UAE Dubai Police General H.Q. General Department of Finance. DFAC has noted that these fines and infringements have been incorrectly posted to ROMAN General Ledger Code 21022 Hire and Other Fees.

Army has paid an historic fine during September, from a fine incurred in May 2012. Due to the lack of action in a timely manner, Defence has so far been unable to locate the responsible driver or member. This fine has not been reimbursed and no member held accountable.



Review	Purpose
<b>Forensic General Ledger Coding Review</b>	<p>The purpose of this review is to provide a level of assurance that Defence's financial information is accurate, that transactions are correctly attributed to either assets liabilities, expense or revenue and expenditure is recorded in the correct GL account. This review provides assurance over the expense groups in ROMAN.</p> <p>To achieve this purpose DFAC analyse ROMAN transactions for selected GL codes with the aim of identity miss-coded transactions. Defence reviewed 26 ROMAN GL codes during the first quarter to 30 September 2016. The results are summarised in the table below.</p> <p>Source: General Ledger Account Codes - <a href="http://intranet.defence.gov.au/find/chart_of_accounts/GLAccountCodes.asp">http://intranet.defence.gov.au/find/chart_of_accounts/GLAccountCodes.asp</a></p>

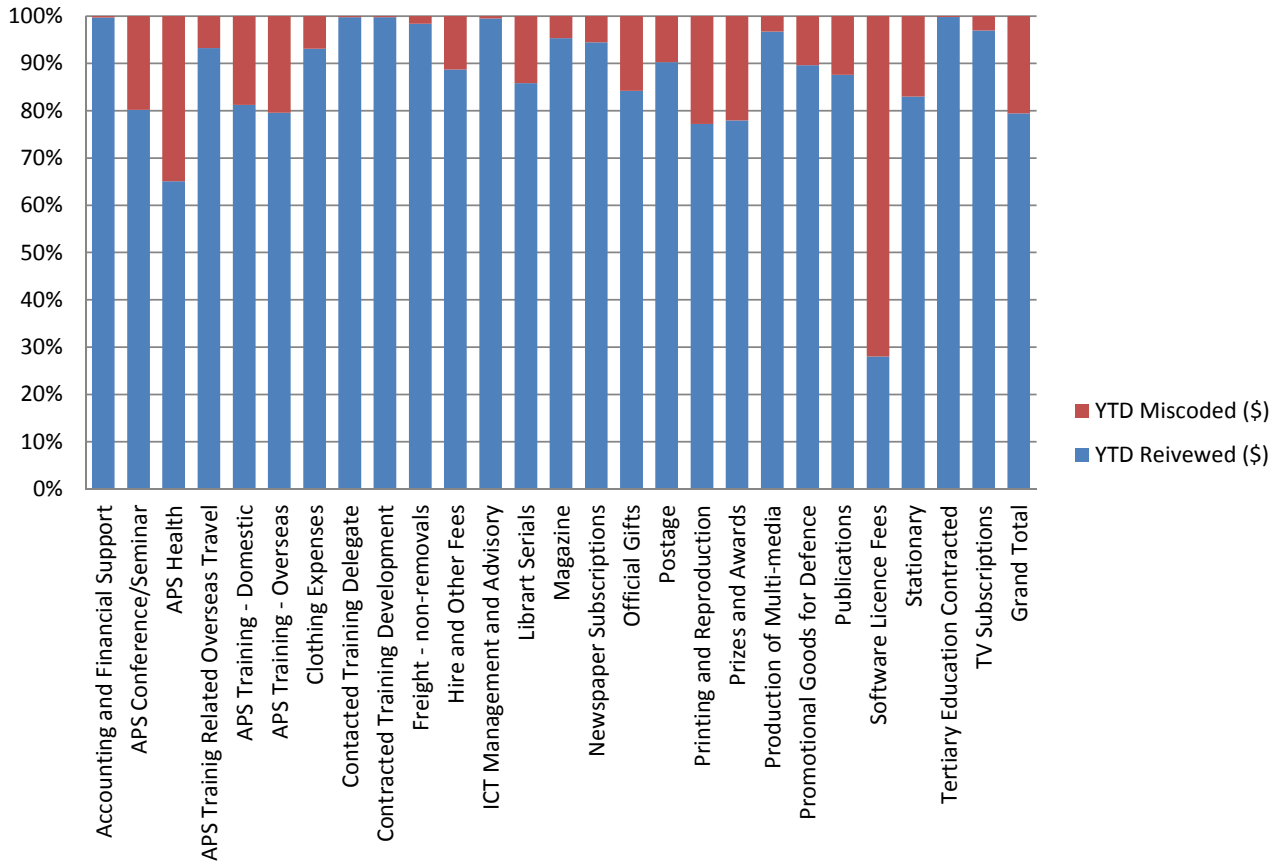
### **Results – Forensic General Ledger Coding Review**

Month	Review Size Transactions (#)	Review Size Dollar Value (\$)	Miscoded Transactions (#)	Miscoded Dollar Value (\$)	Ratio of Miscoding (%)
<b>July – August 2016</b>	18,924	65.99m	2,766	4.7m	<b>16.24</b>
<b>September 2016</b>	10,951	52.9m	1,284	6.5m	<b>12.20</b>
<b>YTD TOTAL 2017</b>	<b>29,875</b>	<b>118.9m</b>	<b>4,050</b>	<b>11.2m</b>	<b>9.45</b>

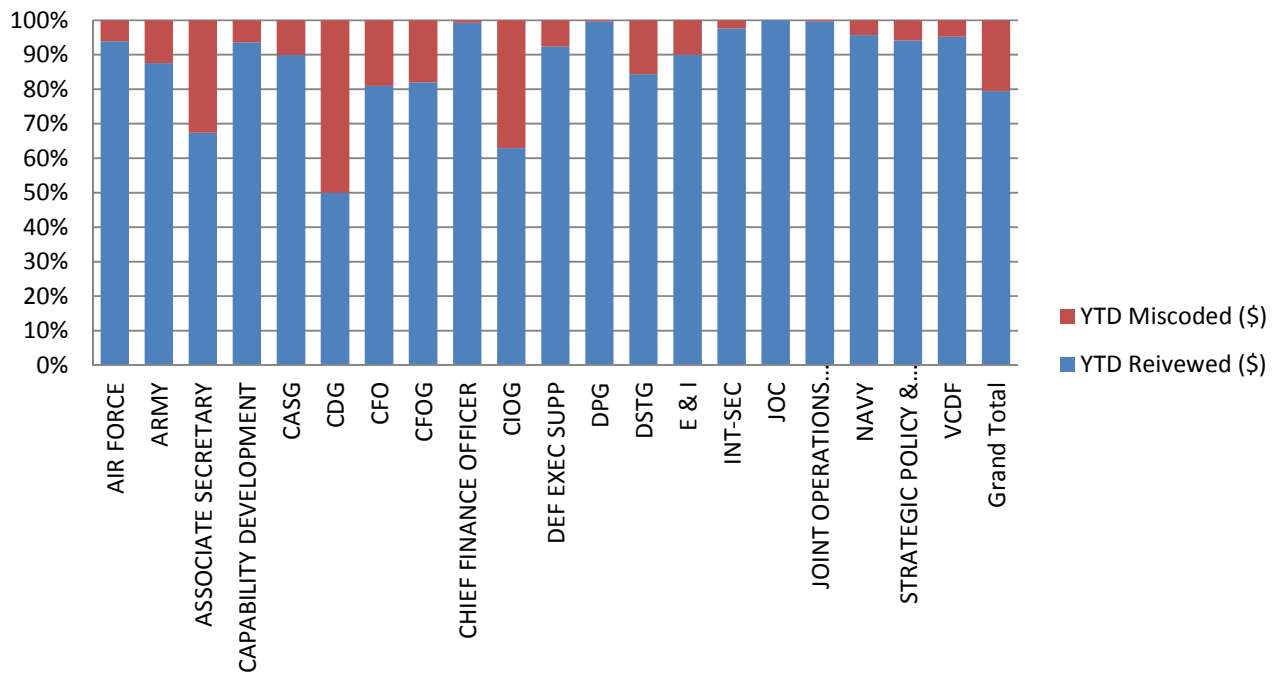
During the review of Defence's ROMAN GL Codes, DFAC concluded the following:

- DFAC reviewed a total of 26 ROMAN GL codes during Quarter 1.
- An unacceptably high error rate of 12.20% was noted for September 2016, bringing the year to date percentage of error by quantity to 9.45%. Incorrect coding can lead to inaccurate reporting, incorrect budgeting and increase the risk of financial misstatement.
- This level of error highlights possible need for re-education amongst Defence member's who enter financial information into Defence's financial systems. It also highlights the need for a review of Defence's GL coding and classifications provided on the FiND website. Many areas have requested more clear and concise guidance and explanations on the FiND website. DFAC is meeting with the Chart of Account team to explore and implement avenues to improve current guidance.
- It is vitally important that Defence has the highest level of confidence in its financial systems and the data within. Supervisors must ensure that expenditure is transacted appropriately, and that all staff inputting data in to ROMAN have sufficient training and available resources. If members are unsure as to how to attribute costs or the GL Look Up on the FiND website, please contact the GL Code mailbox or DFAC staff for assistance.

## ROMAN General Ledger Miscoding Review



## ROMAN General Ledger Miscoding Review



Review	Purpose
<b>Credit Card – High Risk Merchant Review</b>	<p>The purpose of this review is to analyse and review a sample selection of credit card transactions that have been attributed to “High Risk” merchant categories. These merchant categories are set at PoS (Point-of-Sale) by the banks, and Defence review 53 categories including antiques stores, jewellery shops and cigar stands. Defence reviews a sample of transactions in these high risk categories to ensure compliance with Defence expenditure, and to ensure appropriate use of Defence resources.</p> <p><b>DFAC ensures that Defence’s expenditure is appropriate, approved and efficient and effective use of public money. This review minimises the financial risk of credit card fraud or mis-use.</b></p> <p><i>Source: Accountable Authority Instructions Chapter 5. and Defence Procurement Policy Manual Para 53-59 and 63-70.</i></p>

### Results – Credit Card High Risk Merchant Review

Month	Transactions Sampled (#)	Reviewed Transactions (\$)	Transactions Reviewed (#)	Transactions Reviewed (\$)
<b>July – August 2016</b>	131	228,551	82	130,058
<b>September 2016</b>	196	582,350	53	150,643
<b>YTD TOTAL 2017</b>	<b>327</b>	<b>810,900</b>	<b>0</b>	<b>280,701</b>

Month	To be Reviewed (#)	To be Reviewed (\$)	NIL Response (#)	Response Rate (%)
<b>July – August 2016</b>	0	0	49	59.76
<b>September 2016</b>	47	150,721	96	52.00
<b>YTD TOTAL 2017</b>	<b>47</b>	<b>150,721</b>	<b>145</b>	<b>55.66</b>

During the review of Defence's Credit Card High Risk Merchant Review, DFAC noted the following:

- Although DFAC found no intentional mis-use regarding Defence expenditure, DFAC found several concerning issues such as:
  - failure to obtain appropriate delegate approvals;
  - record keeping;
  - using incorrect general ledger; and
  - ignoring expenditure justification.
- As part of expenditure of funds, Defence members must provide sufficient justification. DFAC has noticed members have not completed the justification for expenditure or have wrote very generic responses, for example "The shop was close". Members must at all times be able to justify the expenditure of public monies in efficient, effective, ethical and economical way.

<b>Group</b>	<b>Number of Transactions Miscoded (#)</b>	<b>Number of Transactions Miscoded (\$)</b>	<b>Potential Breach (#)</b>	<b>PGPA Breaches Yet to be Reported (\$)</b>
<b>Air Force</b>	7	3,480	5	1,940
<b>Army</b>	15	101,795	13	7,810
<b>CASG</b>	1	6,275	0	0
<b>CIOG</b>	2	2,589	3	8,167
<b>DPG</b>	0	0	2	11,362
<b>DSTG</b>	1	26	1	1,1562
<b>E&amp;I</b>	0	0	1	6,899
<b>JOC</b>	1	4,590	4	9,547
<b>NAVY</b>	5	2,398	3	3,895
<b>SP&amp;I</b>	0	0	1	-66
<b>VCDF</b>	0	0	3	28,626
<b>YTD TOTAL 2017</b>	<b>32</b>	<b>30,155</b>	<b>36</b>	<b>\$79,745</b>

- It has been noted that some members of the ADF once posted or relocated, no longer have access or copies of supportive documentation and/or documentation has not been appropriately filed. It is the card holder responsibility to locate their own documentation including requesting the documentation from the former unit.
- Some card holders are unaware of the procedures to follow for disputed transactions. Supportive documentation has not been appropriately filed. Documentation regarding fraudulent or incorrect charges must be kept and/or filed.
- Always report unusual or unexpected credit card transactions immediately or in a timely manner. DFAC have reviewed a transaction in which the card holder noticed unexpected transactions (a result of illegal card skimming), however did not complete the appropriate procedure and the card was skimmed multiple times over multiple months prior to any action being taken, including the cancellation of the skimmed card.

Review	Purpose
<b>Compliance Report Testing</b>	<p>Section 19 of the PGPA Act 2013 requires that Defence notify the Minister of all significant non-compliance against the PGPA Act 2013.</p> <p>Non-compliance data is captured through the SharePoint Compliance Reporting Portal. The purpose of this review is to analyse this data, determine the nature of the non-compliance and report on results.</p> <p>The particular focus is on identifying and analysing significant non-compliance.</p> <p>Source: <a href="http://intranet.defence.gov.au/find/policies/compliance_reporting.html">http://intranet.defence.gov.au/find/policies/compliance_reporting.html</a></p>

### Results – Compliance Report Review

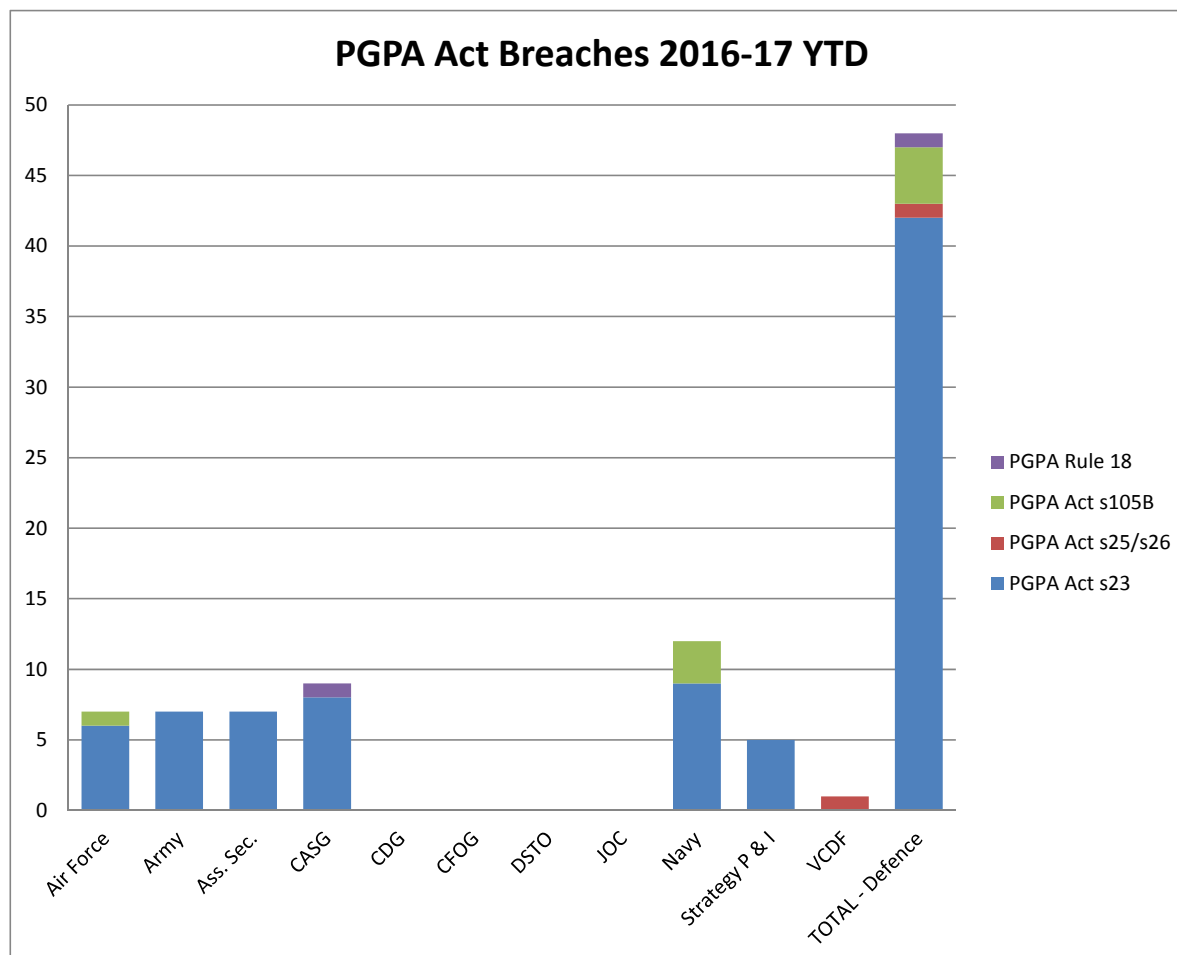
PGPA Breach	Non-Compliance September 2016	Non-Compliance YTD 2016-17
<b>PGPA s23 – Power in relation to arrangements and commitments</b>	18	42
<b>PGPA s25/S26 – Duty of care and due diligence, Duty to act honestly, in good faith and for a proper purpose</b>	1	1
<b>PGPA s105B – Instruments relating to procurement</b>	0	4
<b>PGPA Rule 18 – Approving commitments of relevant money</b>	0	1
<b>Officials PGPA Rule 9</b>	0	0
<b>Total PGPA Non-Compliance - Self Reported*</b>	<b>19</b>	<b>48</b>

\*As per SharePoint Compliance Register (self-reporting).

Please note for detail of Group non-compliance, please view the applicable Group folder in DFAC's *External Parties Folder* in Objective.

Group	PGPA Act s23	PGPA Act s25/26	PGPA Act S105B	PGPA Act Rule 18	Total YTD 2016-17
Air Force	6	0	1	0	7
Army	7	0	0	0	7
Associate Secretary	7	0	0	0	7
CASG	8	0	0	1	9
CDG	0	0	0	0	0
CFOG	0	0	0	0	0
DSTO	0	0	0	0	0
JOC - Army	0	0	0	0	0
Navy	9	0	3	0	12
Strategy Policy	5	0	0	0	5
VCDF	0	1	0	0	1
<b>Total PGPA Breaches</b>	<b>42</b>	<b>1</b>	<b>4</b>	<b>1</b>	<b>48</b>

\*As per SharePoint Compliance Register (self-reporting).





### **Summary of Non-compliance**

- Non –compliance against the PGPA Act totalled 19 reportable instances for September 2016.
- 48 instances of non-compliance have been self-reported during the 2016-17 financial year. 42 instances were reported as non-compliance with s23 of the PGPA Act. These instances occurred as a result of:
  - failures to obtain appropriate delegate approvals prior to entering into or varying an agreement;
  - exceeding delegate approval; and
  - non-compliance related to travel arrangements.
- The four instances of non-compliance reported against PGPA Section 105B, which relates to the failure to use Whole of Government Procurement Guidelines when required.
- The one instance of non-compliance against Section 26 occurred when a Defence official used a Defence Purchase Card for personal purposes. The amount involved was \$15.95, that has since been repaid to Defence..

It is noted that corrective action has been taken against all instances of non-compliance. This mainly involved counselling of staff and providing additional training.

Defence staff have reported a further 37 instances of non-compliance pertaining to the previous financial 2015-16 during the first quarter 2016-17. These instances are not reportable for end of year Compliance Reporting Purposes.

Review	Purpose
<b>CMS Data Review</b>	<p><b>The purpose of this review is to analyse, review and report Defence's use of the corporate card system including expenditure trends.</b></p> <p>DFAC ensures that Defence's financial data is true and accurate.</p> <p>DFAC have developed a testing program designed to improve the forensic/business data analysis work being undertaken by DFAC. DFAC are currently testing expenditure related to taxi usage and cash advances/withdrawals. Assurance and compliance of transactions will commence once streamlined processes for data testing are implemented.</p> <p><i>Source: Accountable Authority Instructions Ch 5. and Defence Procurement Policy Manual Para 53-59 and 63-70.</i></p>

Review	Purpose
<b>Segregation of Duty</b>	<p><b>The purpose of this review is to analyse, review and report Defence's use of the corporate card system including expenditure trends.</b></p> <p>This is to enhance the Financial Controls Framework and Control Testing and ensure Defence's compliance with AASB101.</p> <p>DFAC have reviewed current Segregation of Duty matrix used by CIOG for management of ROMAN user access in order to replace generic risk description with specific description</p> <p>This task ensure that Defence identify and mitigate controls and risk of financial misstatement. Provide advice and ongoing implementation.</p>

- DFAC have reviewed 34 of the 76 Segregation of Duties roles, with 33 roles forwarded to CIOG for comment and advice.
- 28 Risk IDs have been completed. 750 Risk IDs will continue to be reviewed by DFAC.
- With consultation with CFOG-DFO, DFAC have prepared for implementation a semi-annual Defence enterprise wide credit card fraud risk assessment report.
- DFAC have consolidated 11 semi-annual Fraud Risk Assessment reports from 51 Directorates for CFOG. DFAC will review the remaining 5 Fraud Risk Assessment reports. The consolidation process ensures a more efficient and timely reporting during the round as a result of receiving returns from branch heads rather than individual directorates.

Review	Purpose
Gifts, hospitality and sponsorship (GHS)	<p><b>In the past detail of GHS items have been required to respond to Questions on Notice and Senate Estimates briefings. In order to quickly and effectively respond, DFAC established the GHS SharePoint register.</b></p> <p>DFAC staff ensure the completeness and accuracy in GHS reporting by examining all SharePoint entries and conducting completeness reviews.</p> <p>DFAC also run the GHS mailbox, answer ongoing queries and concerns, as well as provides access to the Objective External GHS Folders.</p>

- DFAC answered 8 policy related questions during September.
- DFAC was required to amend 2 separate reported GHS transactions.
- DFAC provided 2 member access to the Objective External GHS Folders.
- DFAC responded to 2 general enquiries regarding GHS.

If you have any enquiries, please email the DFAC's group mailbox at CFO FBI FAC, [cfofbifac@defence.gov.au](mailto:cfofbifac@defence.gov.au). We will respond to enquiry within 2 business days. For specific enquires please see the point of contacts below.

- Late Payments, Defence Credit Cards High Risk Merchant Categories, Invoice Overview, Fines and Infringements, CFOG DREAMS Tokens, CMS potential miscoding: Sandra Cole on (02) 626 54835, [sandra.cole@defence.gov.au](mailto:sandra.cole@defence.gov.au).
- General Ledger Forensic Data Analysis and PGPA Compliance Overview: Michael Sharp (02) 626 5 7455, [michael.sharp4@defence.gov.au](mailto:michael.sharp4@defence.gov.au).

Susan McLean

A/Director Financial Assurance and Compliance

R1-1-B027

02 6265 4136

September 2016

## ANNEX A

### DFAC 2016- 17 Scope and plan for works

DFAC will undertake monthly, quarterly, ad-hoc and yearly reviews in the following areas. DFAC may undertake more or less testing based on Defence's assurance and compliance needs.

Review	Proposed Timing	Purpose
<b>Compliance Report Testing</b>	On-going, monthly	To ensure that Defence complies with the PGPA Act
<b>Gifts, Hospitality and Sponsorship (GHS)</b>	On-going, monthly	To ensure Defence correctly registers and reports GHS, as well as answer QoNs and Senate Estimates.
<b>Forensic GL Reviews</b>	On-going, monthly	To ensure that Defence's financial information is correct and accurate, that all assets are classified correctly and expenditure is appropriate.
<b>Late Payment Review</b>	On-going, monthly	To ensure that Defence meets its financial obligation and to reduce the level of resource wastage and expenditure.  To report on transactions and dollar value of late payments, as well as compliance with processes and procedures.
<b>Reason Code Review</b>	On-going, monthly	To ensure that Defence's financial information is to true and accurate and reflects appropriately.
<b>Credit Card – High Risk Merchant Review</b>	On-going, monthly	To ensure that Defence's expenditure is appropriate, approved and efficient and effective use of public money. This review minimises the financial risk of credit card fraud or mis-use.
<b>Forensic Business Review</b>	Ongoing, monthly	This is to enhance the Financial Controls Framework and Control Testing and ensure Defence's compliance with AASB101.
<b>Defence Financial Controls Framework</b>	Ongoing	This task ensure that Defence identify and mitigate controls and risk of financial misstatement. Provide advice and ongoing implementation.
<b>Fines and Infringements Review</b>	Ongoing, monthly	This task is to ensure that Defence does not incur any fines or infringements on behalf of its members. The review reduces the financial risk of credit card mis-use and the mis-use of public monies.

## **Forensic Analysis**

### Data Analytic Testing

CFO Group continues to improve its forensic data analytic testing program, with Data Analytics Australia (DAA) being engaged to strengthen forensic capabilities and sampling methodologies. DAA is due to complete the first stage of valid statistical sampling methodology by 24 November 2016.

### Key Merchant Categories

In October 2016, there were 60,007 transactions against the 58 Key Merchant Categories. Whilst the majority of these transactions were Qantas Business Travel transactions (i.e. airfares and accommodation), CFO Group are sampling 118 transactions. The review of this sample is still continuing, but no transactions at this stage have required referral to Audit and Fraud Control Division for assessment.

## **Forensic Analysis of Specific Credit Card Transactions**

### iTunes Card Purchases

In October 2016, CFO Group reviewed the use of the Defence Purchasing Card to purchase iTunes software through the Apple store.

Whilst spending approvals were obtained for the purchases, it was inconsistent with Defence's finance policy FINMAN 2 Part 3, whereby approval is required by CIO Group for all software procured, including iTunes.

Out of the 19 transactions reviewed by CFO Group, 10 do not comply with Defence's financial policy.

Breakdown of iTunes transactions and Non-Compliance by Group is as follows:

<b>Group</b>	<b>Number Sampled</b>	<b>Reviewed \$</b>	<b>Awaiting Response</b>	<b>Non-Compliances</b>	<b>Non-Compliance \$</b>
Air Force	10	3,234.44	2	6	2,576.42
Army	4	35.51	0	3	31.02
CIOG	3	7,641.00	0	0	0
DSTG	1	6.47	1	0	0
Navy	1	7.99	0	1	7.99
<b>Grand Total</b>	<b>19</b>	<b>10,925.41</b>	<b>3</b>	<b>10</b>	<b>2,615.43</b>

For example: In one instance, a Defence member's son used the Defence credit card twice to make multiple iTune transactions. The member has been advised of the non-compliance and has repaid the money.

Another instance, approval was sought from CIO Group but was denied, however the VCDF Group Unit continued with the purchase irrespectively. The Unit has been advised of the non-compliance and that the requirement to adhere to Defence's financial management policy.

### Traffic Infringements

As the Committee was advised last month, 121 traffic infringements relating to hire or rental vehicles were being investigation. In October, a further 21 fines were being identified. The table below outlines the number of Traffic Infringements for hire and rental vehicles.

Table – Traffic Infringements for the Period July to October 2016

<b>Group</b>	<b>Not yet repaid</b>	<b>Repaid</b>	<b>Invoice raised but payment not yet received</b>	<b>Review not complete</b>	<b>Total</b>
ARMY	1	2	1	-	4
JOC		118	15	-	133
Navy		1		-	1
Being Investigated				4	4
<b>Total</b>	<b>1</b>	<b>121</b>	<b>16</b>	<b>4</b>	<b>142</b>
<b>\$ Value</b>	<b>\$90.91</b>	<b>\$18,403.59</b>	<b>\$2,587.27</b>	<b>\$5,248.00</b>	<b>\$26,329.77</b>

In addition to the fines and infringements listed above, CFO Group was provided with data held by Defence Commercial Vehicles (CASG), for Defence owned and leased vehicles.

Since 1 July 2016, an additional 288 fines and infringements for Defence owned and leased vehicles have been identified. Of the 288 fines, 241 fines have had the appropriate declaration completed to pass the liability onto the driver, with the remaining 47 fines being pursued by Commercial Vehicles in CASG. The following table outlines the number of fines by state.

<b>State</b>	<b>Total Number of Fines Still being Investigated</b>	<b>Total Number of Fines Closed</b>	<b>TOTAL Number of Fines</b>
ACT	0	0	0
NSW	4	75	79
NT	2	6	8
QLD	19	70	89
SA	0	1	1
VIC	22	89	111
<b>TOTALS</b>	<b>47</b>	<b>241</b>	<b>288</b>

### Taxi Fares

Three rounds of testing on taxi fares over \$200 were conducted in October, which included a total of 253 transactions with a total value of \$83,894.

Out of the 253 transactions, 133 reviews have been completed. Of these 133 taxi fares, 129 transactions require no further action, 4 transactions exceeded the approved travel budget. There are still 90 taxi fare transactions awaiting documentation and 30 taxi fare responses to be reviewed.

The 253 taxi fare transactions have been appropriately approved and are for Conditions of Service and/or business related travel.

**Taxi related transactions >\$200 (by Group)**

	Transactions	Total Amount	Average Amount
ARMY	24	\$11,853	\$494
CASG	32	\$12,015	\$375
CIOG	2	\$584	\$292
DES	2	\$479	\$239
DPG	7	\$1,606	\$229
DSTG	2	\$557	\$279
E&IG	6	\$1,952	\$325
JOC	4	\$847	\$212
NAVY	41	\$13,678	\$334
RAAF	111	\$27,880	\$251
SPIG	7	\$4,749	\$678
VCDF	15	\$7,696	\$513
<b>Grand Total</b>	<b>253</b>	<b>\$83,894</b>	<b>\$332</b>

**Department of Defence****DEFGRAM 613/2016****Issue Date: 08 December 2016****Expiry Date: 10 March 2017**

---

**USE OF DEFENCE TRAVEL CARD FOR JOINT OPERATIONS  
COMMAND OPERATIONS AND EXERCISES****Purpose**

1. The purpose of this Defgram is to inform personnel of a trial to use the Defence Travel Card (DTC) in lieu of Cabcharge etickets for travel associated with Joint Operations Command (JOC) led operations and exercises.

**Approved method of payment**

2. Chief of Joint Operations Command (CJOPS) has directed that a trial be conducted over the period December 2016 to March 2017 whereby DTC is to be used to pay for ground transport services associated with JOC operations and exercises.

**Transition period arrangements**

3. From 12 December 2016 all members who are participating in a JOC sponsored operation or exercise will be required to use their DTC as the preferred method of payment for ground transport. Following the end of the trial period, 1JMOVGP will engage the Service Headquarters, JTF633 and principal stakeholders to ascertain any issues. For personnel already deployed and not in possession of their DTC, Cabcharge etickets will be made available by Joint Movement Control Offices, on their return to Australia.

**Application**

4. Movement Orders (MOVORDS) will include a Section 23 Delegate approval statement with clear direction on the conditions of DTC use, maximum limit and details of the Cost Centre Code and Fund Numbers to be utilised.

5. In addition, the statement will include information on Account Holder access and the transfer of functionality to a parent unit representative to acquit transactions when a member is unable to access the Defence Protected Network. The member's parent/posted Unit (or Admin Unit) will retain responsibility for ensuring they, or the member, acquit the CMS transaction.

6. Cabcharge etickets will remain available to be issued by Joint Movement Control Offices in exceptional circumstances.



**UNCLASSIFIED**

2

7. Further information on the use of DTC for JOC operations and exercises can be obtained from 1st Joint Movement Group (1JMOVGP) Operations and Exercises Cell via email at [hq1jmovgp.operations@defence.gov.au](mailto:hq1jmovgp.operations@defence.gov.au) or from the Contact Officer below.

**IG Murray**

Commodore, Royal Australian Navy  
Director General Support  
Joint Operations Command

**Contact Officer:**

**MAJ Lucas Jahne**

SO2 OPS

Telephone:

Email:

**UNCLASSIFIED**



## DFAC Defence Credit Card Monitoring and Controls Program - Tracking workbook

Organisation and accr				Transaction Information		Merchant information		Amount	Test information		Sample status			DFAC assessment and review		
Defence_Group	Transaction_Date	Create_Date	Card_Type	Transaction_Description	Merchant_Category	Amount	Test_Data_Period	Test_Name	Date_Requested	Date_Due_Original	Date_Due_Updated	Status_Party	Status_Calculated	Review_Tester	Review_Started	
CASG	1/11/2016	2/11/2016	Diners	PV LIMOUSINES	Limousines and Taxicabs	\$232.31	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
CASG	1/11/2016	2/11/2016	Diners	PV LIMOUSINES	Limousines and Taxicabs	\$240.31	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
CASG	3/11/2016	4/11/2016	Diners	TAXI EXCHANGE MELB	Limousines and Taxicabs	\$241.50	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
CASG	31/10/2016	1/11/2016	Diners	AUSTRALIA WIDE CHAUFFEUR	Limousines and Taxicabs	\$268.00	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
CASG	1/11/2016	4/11/2016	MasterCard	CORPORATE CARS AUS PL	Limousines and Taxicabs	\$813.92	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
CASG	25/10/2016	31/10/2016	MasterCard	USD 180 00 AT 1 3170	Limousines and Taxicabs	\$237.07	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
CASG	25/10/2016	31/10/2016	MasterCard	USD 200 00 AT 1 3170	Limousines and Taxicabs	\$263.41	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
CASG	28/10/2016	2/11/2016	MasterCard	USD 305 50 AT 1 3321	Limousines and Taxicabs	\$406.98	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
CIOG	29/10/2016	1/11/2016	Diners	TAXIEPAY	Limousines and Taxicabs	\$295.26	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
CIOG	29/10/2016	1/11/2016	Diners	TAXIEPAY	Limousines and Taxicabs	\$288.60	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
JOC	28/10/2016	1/11/2016	Diners	TOTAL FARE INCL GST 206 85 to	Limousines and Taxicabs	\$206.85	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
NAVY	2/11/2016	3/11/2016	Diners	INGOGO PTY LTD	Limousines and Taxicabs	\$210.00	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
NAVY	2/11/2016	4/11/2016	Visa	TAXI EPAY LIMOS EDGECLIFF	TAXICABS LIMOUSINE HIRE	\$3,291.22	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
NAVY	28/10/2016	31/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$256.94	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
NAVY	31/10/2016	1/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$238.88	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
NAVY	2/11/2016	4/11/2016	Diners	TOTAL FARE INCL GST 304 50 to	Limousines and Taxicabs	\$304.50	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
NAVY	2/11/2016	3/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$204.44	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
NAVY	28/10/2016	31/10/2016	Diners	ATLAS LIMOUSINES SER	Limousines and Taxicabs	\$416.00	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
RAAF	29/10/2016	1/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$257.25	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	30/10/2016	1/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$237.30	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016	15/12/2016	Card_or_Account_Holder	Awaiting_Reply	Edward	24/11/2016	
RAAF	2/11/2016	3/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$220.44	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	28/10/2016	31/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$229.84	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	28/10/2016	31/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$244.20	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016	16/11/2016	Card_or_Account_Holder	Complete	Edward	15/11/2016	
RAAF	28/10/2016	31/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$210.00	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	28/10/2016	31/10/2016	Diners	TAXIEPAY	Limousines and Taxicabs	\$220.63	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	2/11/2016	3/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$220.50	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	28/10/2016	31/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$280.19	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
RAAF	31/10/2016	2/11/2016	Diners	TOTAL FARE INCL GST 204 75 to	Limousines and Taxicabs	\$204.75	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	3/11/2016	4/11/2016	Diners	HAWKESBURY SHUTTLE S	Limousines and Taxicabs	\$490.00	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	15/11/2016	
RAAF	2/11/2016	3/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$220.50	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	2/11/2016	3/11/2016	Diners	PREMIER TRANSFER	Limousines and Taxicabs	\$350.20	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	15/11/2016	
RAAF	1/11/2016	2/11/2016	Diners	PV LIMOUSINES	Limousines and Taxicabs	\$207.18	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	3/11/2016	4/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$272.56	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Awaiting_Review	Edward	24/11/2016	
RAAF	30/10/2016	1/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$236.09	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	3/11/2016	4/11/2016	Diners	BRISBANE PREMIER LIMO SER	Limousines and Taxicabs	\$299.57	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016	31/12/2016	Card_or_Account_Holder	Awaiting_Reply			
RAAF	27/10/2016	31/10/2016	Diners	TOTAL FARE INCL GST 233 10 to	Limousines and Taxicabs	\$233.10	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
RAAF	29/10/2016	1/11/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$220.50	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
RAAF	2/11/2016	3/11/2016	Diners	PREMIER TRANSFER	Limousines and Taxicabs	\$412.00	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
VCDF	31/10/2016	2/11/2016	Diners	TOTAL FARE INCL GST 210 90 to	Limousines and Taxicabs	\$210.90	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
VCDF	31/10/2016	1/11/2016	Diners	AUSTRALIA WIDE CHAUFFEUR	Limousines and Taxicabs	\$228.00	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Overdue			
VCDF	27/10/2016	31/10/2016	Visa	AERIAL TRANSPORT CONSO FYSH	TAXICABS LIMOUSINE HIRE	\$316.50	2016.10.31 - 2016.11.06	Taxi > \$200	8/11/2016	10/11/2016		Card_or_Account_Holder	Complete	Edward	14/11/2016	
ARMY	21/10/2016	24/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$214.62	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	15/11/2016	
ARMY	26/10/2016	27/10/2016	Diners	GOLD CROWN LIMOUSINES	Limousines and Taxicabs	\$320.00	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	16/11/2016	
ARMY	21/10/2016	25/10/2016	Diners	TOTAL FARE INCL GST 223 02 to	Limousines and Taxicabs	\$223.02	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
ARMY	21/10/2016	25/10/2016	Diners	TOTAL FARE INCL GST 207 32 to	Limousines and Taxicabs	\$207.32	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
ARMY	21/10/2016	25/10/2016	Diners	TOTAL FARE INCL GST 202 07 to	Limousines and Taxicabs	\$202.07	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
ARMY	26/10/2016	28/10/2016	Visa	CABCHARGE AUSTRALIA SYDNI	TAXICABS LIMOUSINE HIRE	\$344.16	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Usha	23/11/2016	
ARMY	27/10/2016	28/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$201.60	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	10/11/2016	
ARMY	27/10/2016	28/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$233.99	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
ARMY	21/10/2016	24/10/2016	Diners	OMNICAR AUSTRALIA	Limousines and Taxicabs	\$309.30	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
CASG	26/10/2016	27/10/2016	Diners	PV LIMOUSINES	Limousines and Taxicabs	\$240.31	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Usha	10/11/2016	
CASG	26/10/2016	27/10/2016	Diners	ATLAS LIMOUSINES SER	Limousines and Taxicabs	\$280.00	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
CASG	26/10/2016	27/10/2016	Diners	SIT CARS TAXIS	Limousines and Taxicabs	\$215.61	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	15/11/2016	
CASG	27/10/2016	28/10/2016	Diners	SIT CARS TAXIS	Limousines and Taxicabs	\$220.34	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	15/11/2016	
CASG	26/10/2016	27/10/2016	Diners	PV LIMOUSINES	Limousines and Taxicabs	\$210.79	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
CASG	26/10/2016	27/10/2016	Diners	PV LIMOUSINES	Limousines and Taxicabs	\$259.00	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
CASG	26/10/2016	27/10/2016	Diners	PV LIMOUSINES	Limousines and Taxicabs	\$265.31	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
DES	26/10/2016	27/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$205.35	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	15/11/2016	
DPG	27/10/2016	28/10/2016	Diners	TAXIEPAY	Limousines and Taxicabs	\$239.76	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
DPG	21/10/2016	24/10/2016	Diners	KS LIMOUSINES	Limousines and Taxicabs	\$225.50	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
E&IG	20/10/2016	24/10/2016	Visa	BAYVIEW TAXIS FRANKSTON	TAXICABS LIMOUSINE HIRE	\$770.00	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	24/11/2016	
JOC	25/10/2016	27/10/2016	Diners	TOTAL FARE INCL GST 204 33 to	Limousines and Taxicabs	\$204.33	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Overdue			
NAVY	26/10/2016	28/10/2016	Diners	TOTAL FARE INCL GST 210 00 to	Limousines and Taxicabs	\$210.00	2016.10.24 - 2016.10.30	Taxi > \$200	1/11/2016	4/11/2016		Card_or_Account_Holder	Complete	Edward	15/11/2016	
NAVY	25/10/2016	26/10/2016	Diners	GM CABS AUSTRALIA	Limousines and Taxicabs	\$231.00	2016.10.24									





**From:** Baker, Susan MS 1 **On Behalf Of** Defence Credit Cards  
**Sent:** Tuesday, 29 November 2016 08:55  
**Subject:** [SEC=UNCLASSIFIED]

**UNCLASSIFIED**

Dear Card Holder,

Card records indicate that you have been sent a Defence Travel Card or Companion Mastercard but have failed to activate it within 60 days.

As part of necessary controls on the issue of cards it is now practice to cancel cards that have not been activated within 90 days.

From the date of sending this message you will have 30 days to activate your card before it is cancelled.

If your card is not activated by COB 29/12/2016 your DTC or Companion Mastercard will be cancelled.

Once cancelled you will need to **reapply** for a new Defence Travel Card or Companion Mastercard should you have a requirement to travel for Defence business.

If you require your Defence Travel Card or Companion Mastercard, activate it by calling **1300 306 103** and follow the prompts.

If you have **NOT** received your card please contact Diners **Premium Services Delivery Team on 1800 105 660** to arrange a replacement.

**PLEASE DO NOT REPLY TO THIS EMAIL UNLESS YOU HAVE AN ISSUE - THIS PROCESS IS AUTOMATED AND REQUIRED BY AUDIT**

**Defence Credit Cards**  
[defence.CreditCards@defence.gov.au](mailto:defence.CreditCards@defence.gov.au)

**Susan Baker**  
Finance Officer  
Directorate of Financial Operations  
Chief Finance Officer Group  
Department of Defence

| PO Box 7901 | Russell Offices  
CANBERRA BC | ACT 2610

UNCLASSIFIED



Australian Government  
Department of Defence

AE 602  
Revised 27 Oct 16

## Corporate Card Application and Limit Amendment

### I am applying for

- ☒ Defence Travel Card
- ☐ Companion MasterCard
- ☐ Both Defence Travel Card and Companion MasterCard
- ☐ Defence Purchasing Card
- ☐ Change to Defence Travel Card credit limit
- ☐ Change to Defence Purchasing Card credit limit

### Agreement statement

#### Please read the following before applying for a Defence Travel Card.

By completing an application for a Defence Travel Card (*hereinafter referred to as the DTC*) I acknowledge that I have read, understood and agree to the following conditions under which the DTC will be issued in my name:

- I will not use my DTC, nor permit it to be used, for other than official purposes.
- The use of the DTC is subject to the procedures outlined in the [Defence Travel Card fact sheet](#).
- I am required at all times to take strict care of the DTC and PIN and, in the event that my negligence may lead to the loss of the DTC and or PIN, then the provision of [AAIs 5.2.4.1](#) may be invoked.
- If the DTC is lost, stolen or destroyed, I am to report it immediately to the card provider and [Defence Credit Cards](#).
- I understand that it is illegal to use the card other than in accordance with the instructions given to me. If I misuse the card I may be charged, and if found guilty, I may be severely punished, including imprisonment.

- ☒ I acknowledge and agree to the above conditions before I complete this application.
- ☒ I confirm my postal address and contact details are correct in the Defence Corporate Directory and my application may be rejected or inhibit the delivery of my card if these are incorrect.

- ☒ I am filling in this form on a DRN workstation.  
*Note: Please untick this box if you are on the Next Gen Desktop environment.*

### DTC application details

#### Employee details

Employee ID *	Title *	Family name *	Given name(s) as on PMKeyS *
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
DOB (over 18) *	Gender	Group *	CMS account holder *
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- ☐ I require an unbranded card for operational reasons

Select your work email address domain \*

- ☐ Defence ☐ DSTG ☐ Fleet ☐ F05 Navy ☐ Defence Computing Bureau

Work email address

#### Account assignment \*

Company code *	Cost centre *	WBS	Internal order	Fund
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>



UNCLASSIFIED

**UNCLASSIFIED**

**DTC applicant signature**

Signature \*

If you cannot digitally sign, click [here](#) for guidelines on how to resolve your issue or contact Corporate Cards Support Centre for additional DTC support.



**UNCLASSIFIED**

ACCOUNTABLE AUTHORITY INSTRUCTION 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

## ACCOUNTABLE AUTHORITY INSTRUCTION

### 5 COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

#### 5.1 INTRODUCTION

##### 5.1.1 About this Accountable Authority Instruction (AAI)

5.1.1.1 This AAI is issued under section 20A of the PGPA Act. It provides instruction to officials about the use of Commonwealth credit cards and credit vouchers.

##### 5.1.2 What are Commonwealth credit cards and credit vouchers?

5.1.2.1 A Commonwealth credit card is a credit card issued to the Commonwealth entity to enable it to obtain cash, goods or services on credit (i.e. with payment deferred). A credit voucher, in a sense, is a paper based credit card that generally comes with an attached spending limit (e.g. a Cabcharge voucher).

5.1.2.2 Charge cards and vendor cards issued to Defence are both a form of Commonwealth credit card for the purposes of the PGPA Act.

- a) Charge cards authorise the holder to buy goods or services on credit, with payment in full required to be made at a later date (e.g. Diners card).
- b) Vendor cards (sometimes called "limited-purpose purchase cards") are charge cards provided by specific retailers (e.g. Cabcharge cards).

5.1.2.3 Commonwealth credit cards and credit vouchers are different from personal credit cards or vouchers, as they do not provide the holder with a revolving line of credit. Money borrowed by Defence through the use of a credit card or credit voucher must be paid in full within a specific timeframe.

5.1.2.4 Debit cards, pre-paid credit cards and gift vouchers issued to Defence are not Commonwealth credit cards. They should be treated as if they were relevant money.

##### 5.1.3 How do Commonwealth credit cards and credit vouchers work?

5.1.3.1 The use of a Commonwealth credit card or credit voucher is a borrowing by Defence (i.e. an advance of money that must be repaid in accordance with contractually agreed terms).

5.1.3.2 The Finance Minister can enter into a limited range of borrowing agreements under section 56 of the PGPA Act. This includes entering into an agreement for the issue to, and use by, the Commonwealth of credit cards or credit vouchers, provided that the agreement requires the money borrowed to be repaid within 90 days. The Finance Minister has delegated this power to the Secretary, who in turn, has delegated these powers to limited Defence officials under FINMAN 2 Schedule 6.

##### 5.1.4 References

5.1.4.1 [Public Governance, Performance and Accountability Act 2013](#), sections 15 and 56

5.1.4.2 [Commonwealth Procurement Rules](#)

5.1.4.3 [ANAO Report 37: Management of Credit Cards](#)

5.1.4.4 [DI\(G\) ADMIN 45-2](#) *The reporting and management of notifiable incidents*

5.1.4.5 FINMAN 5 - Financial Management Manual, Chapter 5 *Commonwealth Credit Cards and Credit Vouchers*

5.1.4.6 [FINMAN 2](#) - Financial Delegations Manual, schedules 1, 2 and 6

#### 5.2 WHAT ARE COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS?

5.2.1.1 Commonwealth credit cards are cards (or virtual cards) issued to obtain goods or services on credit.

5.2.1.2 Credit vouchers are single use documents (including electronic ones) that allow to obtain goods or services on credit (e.g. a Cabcharge voucher).

ACCOUNTABLE AUTHORITY INSTRUCTION 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

- 5.2.1.3** Debit cards, pre-paid credit cards and gift vouchers are not Commonwealth credit cards. They must be treated as if they were relevant money.

**5.3 HOW DO COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS WORK?**

- 5.3.1.1** Purchases made via a Commonwealth credit card or credit voucher are borrowings for the purpose of section 56 of the PGPA Act.

**Instructions – All officials**

<b>5.3.1.2</b>	Only the person issued with a Commonwealth credit card or credit voucher, or someone specifically authorised by that person, may use that credit card, credit card number or credit voucher.
<b>5.3.1.3</b>	You must comply with the instructions relating to the issue, use and disposal of Commonwealth credit cards on <a href="#">Corporate Card Support Website</a> .
<b>5.3.1.4</b>	Only specifically authorised personnel may use Commonwealth Corporate Travel System (CTS) accounts (i.e. virtual cards).
<b>5.3.1.5</b>	You must not enter into a credit card agreement unless you are a delegate under FINMAN 2 schedule 6.
<b>5.3.1.6</b>	You must report fraudulent or suspected fraudulent use of a Commonwealth credit card or credit voucher to the Defence Investigative Authority in accordance with DI(G) Admin 45-2 <i>The reporting and management of notifiable incidents</i> .
<b>5.3.1.7</b>	You must ensure that any Commonwealth credit card and/or credit voucher issued to you is stored safely and securely.
<b>5.3.1.8</b>	You must ensure that any PIN issued with a Commonwealth credit card is not stored with the Commonwealth credit card.
<b>5.3.1.9</b>	You must only use a Commonwealth credit card, card number or credit voucher to obtain cash, goods or services for official Commonwealth purposes.
<b>5.3.1.10</b>	In deciding whether to use a Commonwealth credit card or credit voucher, you must consider whether it would be the most cost-effective payment option in the circumstances.
<b>5.3.1.11</b>	Before using a Commonwealth credit card or credit voucher, you must ensure that the requirements in AAI 2 - <i>Approval and Commitment of Relevant Money</i> , have been met before entering into the arrangement.
<b>5.3.1.12</b>	You must ensure that your use of a Commonwealth credit card or credit voucher is consistent with the approval given, including any conditions of the approval.
<b>5.3.1.13</b>	You must acquit transactions within 60 days of the transaction being recorded in the Card Management System (CMS).
<b>5.3.1.14</b>	Private expenditure must only be paid using a Commonwealth credit card where: <ul style="list-style-type: none"><li>a) It is necessary, unavoidable, directly linked with and coincidental to expenditure for official Commonwealth purposes; and</li><li>b) You have prior FINMAN 2 schedule 1 delegate approval.</li></ul>
<b>5.3.1.15</b>	Where a Commonwealth credit card has been used for private expenditure, the card holder must repay the amount of the private expenditure prior to verification of the expenditure within the CMS. The verification period within the CMS is a maximum of 30 days.
<b>5.3.1.16</b>	If a transaction is disputed, you must adhere to the disputed transactions process as outlined in the <i>Transaction Queries and Disputes with Card Providers Task Card</i> on the <a href="#">Corporate Card Support Website</a> .



ACCOUNTABLE AUTHORITY INSTRUCTION 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

**Instructions – Group Heads**

<b>5.3.1.17</b>	You, or your nominated representative must review Commonwealth credit card credit limit levels as risk assessments determine. The maximum time between reviews is 12 months.
-----------------	--

**5.3.2 Instructions – Officials with a delegation to enter into borrowing agreements for Commonwealth credit cards and credit vouchers**

<b>5.3.2.1</b>	<p>When entering into a borrowing agreement for the issue to, and use by, the Commonwealth entity of credit cards or credit vouchers, you must:</p> <ul style="list-style-type: none"><li>a) have a valid delegation under FINMAN 2 schedule 6 to enter into borrowing agreements;</li><li>b) ensure that the requirements in AAI 2 - <i>Approval and Commitment of Relevant Money</i> have been met;</li><li>c) ensure that the procurement of the credit card and/or credit voucher services is in accordance with the CPRs (see AAI 3 - <i>Procurement</i>); and</li><li>d) ensure that the borrowing agreement requires the money borrowed to be repaid within 90 days of the Commonwealth being notified of the amount borrowed.</li></ul>
----------------	---

**UNCONTROLLED IF PRINTED  
UNCLASSIFIED**

**Department of Defence**

**DEFGRAM 461/2016**

**Issue Date: 29 September 2016**  
**Expiry Date: 06 January 2017**

---

**CARD MANAGEMENT SYSTEM - REMOVAL OF SUPERVISOR  
APPROVAL FOR DEFENCE CREDIT CARDS**

**Purpose**

1. The Enterprise Business Committee (EBC) has agreed that from 15 October 2016, there will no longer be a requirement for CMS Supervisors to approve Defence credit card transactions in CMS. This includes both Defence Purchasing Cards (DPC) and Defence Travel Cards (DTC). Follow up communication through DEFGRAM and Group and Service communication channels will follow in the next few days.
2. As a result of this decision any transactions in CMS awaiting Supervisor approval on 15 October 2016 will automatically be approved.
3. Note that DTC refers to both the Diners Card and the MasterCard Companion Card.

**Background**

4. The Review of Red Tape in Defence delivered by Dr Alan Thomas in August 2015 recommended a range of actions be completed in order to make Defence processes more streamlined and efficient. The Review looked at "ways to reduce or eliminate those processes Defence has imposed on itself above and beyond what has been mandated by central agencies or legislation."
5. Removing the requirement for CMS Supervisors to approve Defence credit card transactions in CMS is the first step in addressing travel related recommendations from the Review. Further streamlining will be undertaken as part of the implementation of the new Defence travel and expense management system.

**New Travel Process (DTC)**

**Approving Expenditure**

6. When using a Defence credit card, expenditure must be approved by a FINMAN 2 Division 1, Schedule 1 delegate prior to committing the Commonwealth, including booking travel, or any other travel related costs, e.g. flights, accommodation, passports, visas, third party notes, etc.
7. The FINMAN 2 Division 1 delegate's approval for travel should be documented on the appropriate record depending on the type of travel undertaken. For example:
  - a. iTravel;
  - b. Overseas Travel Budget Calculator;

**UNCLASSIFIED**

**UNCONTROLLED IF PRINTED  
UNCLASSIFIED**

2

- c. Excel spreadsheet based travel budget calculators; or
- d. AE505 Travel Request Form.

**After Undertaking Travel**

- 8. FINMAN 5 will be updated to take effect from 15 October 2016 to reflect updated travel processes.
- 9. Upon completion of official travel, travellers will only be required to complete the after travel certification where there is a change to the approved travel plan that:
  - a. increases the original budget, this requires additional financial delegate approval is required; or
  - b. decreases the original budget and results in an amount needed to repaid.
- 10. Defence credit card transactions must still be acquitted by the account holder through CMS within 60 days of a transaction appearing on CMS in accordance with Accountable Authority Instruction (AAI) 5.3.1.13.
- 11. Once Defence credit card transactions are acquitted on CMS, they will automatically be approved in the system.
- 12. Account holders will no longer be required to print and sign the CMS Expense Summary Report once transactions have been processed through CMS.

**Diners Card Documentation**

- 13. In accordance with FINMAN 5.2.6.4, transactions carried out using a Diners Card meet the Australian Taxation Office (ATO) requirements to claim Goods and Services Tax (GST) and therefore hard copies of invoices and receipts related to these transactions are not required to be retained.
- 14. Receipts are not required for cash withdrawals using the Diners Card for meals and incidentals. However, where cash is withdrawn for other travel costs, receipts are required for GST redemption and verification.
- 15. The relevant approved travel budget calculator and associated travel documentation must be retained on an official file in accordance with FINMAN 5.1.6.3. It must remain easily accessible for 7 years from the end date of travel; the exception to this is the receipts required for cash withdrawals as per paragraph 14.

**MasterCard Companion Card Documentation**

- 16. Unlike the Diners Card, the MasterCard Companion Card does not meet ATO GST requirements; therefore, all invoices and receipts relating to a domestic transaction on the MasterCard must be retained and filed in accordance with the Records Management Policy Manual (RECMAN).

**UNCLASSIFIED**

**UNCONTROLLED IF PRINTED  
UNCLASSIFIED**

3

**New Expense Process (DPC)**

**Approving Expenditure**

17. When using a Defence purchasing credit card, expenditure must be approved by a FINMAN 2 Division 1, Schedule 1-6 delegate prior to committing the Commonwealth.

18. The FINMAN 2 Division 1 delegate's approval for expenditure should be documented on the appropriate record depending on the expenditure undertaken. For example:

- a. AE643 Defence Purchasing Form; or
- b. AC977 Credit Card Authorisation Form

**After Completing Purchase**

19. FINMAN 5 will be updated to take effect from 15 October 2016 to reflect updated expense card processes.

20. Defence credit card transactions must still be acquitted by the account holder through CMS within 60 days of a transaction appearing on CMS in accordance with Accountable Authority Instruction (AAI) 5.3.1.13.

**MasterCard DPC Documentation**

21. The DPC MasterCard Card does not meet ATO GST requirements; therefore, all invoices and receipts relating to transaction on the DPC MasterCard must be retained and filed in accordance with the Records Management Policy Manual (RECMAN).

**General Information**

**Role of CMS Supervisors**

22. CMS Supervisors will:
- a. no longer be required to check and approve cardholder's transactions on CMS; and
  - b. retain visibility of their staffs' CMS profile and will still have responsibility for ensuring their staff process CMS transactions within 60 days of appearing on CMS. Emails will continue to be sent to CMS Supervisors notifying them of their staffs' outstanding CMS transactions.

**Forensic Monitoring and Controls**

23. In line with the Public Governance, Performance and Accountability Act (PGPA) 2013 cardholders should be aware that the controls, assurance activities and compliance checks conducted by Directorate of Financial Assurance and Compliance (DFAC), Chief Finance Officer Group (CFOG) will continue. These controls are in place to deal with fraud, as opposed to legitimate additional expenditure incurred by employees that could not have been anticipated prior to travel.

**UNCLASSIFIED**

UNCONTROLLED IF PRINTED  
**UNCLASSIFIED**

4

24. This means that at any time you may be required to provide your travel documentation to DFAC for review.

**Additional Information**

25. Guidance on the processes that should be followed for Defence credit cards can be found in the task cards on the Corporate Cards Support Centre intranet page <http://drnet.defence.gov.au/FinD/CCSC/Pages/default.aspx>

26. Corporate Travel System (CTS) accounts or other Defence credit cards already setup to have transactions automatically approve on CMS once acquitted by the account holder will continue to do so.

**Contacts**

27. Account holders should contact the Corporate Card Support Centre in the first instance with any issues or questions regarding the new process through the email address [corporate.cards@defence.gov.au](mailto:corporate.cards@defence.gov.au).

Alternatively contact your relevant Group Chief Finance Officer (GCFO) listed on the intranet [http://intranet.defence.gov.au/find/cfo\\_group/cfo\\_org\\_chart.html](http://intranet.defence.gov.au/find/cfo_group/cfo_org_chart.html)

**David Spouse**

First Assistant Secretary Financial Services  
Chief Finance Officer Group

**UNCLASSIFIED**

DEPARTMENT OF DEFENCE  
SEC 2015-001

FINANCIAL FRAMEWORK (SUPPLEMENTARY POWERS) ACT 1997  
PUBLIC GOVERNANCE, PERFORMANCE AND ACCOUNTABILITY ACT 2013  
PUBLIC GOVERNANCE, PERFORMANCE AND ACCOUNTABILITY RULE 2014  
JUDICIARY ACT 1903

INSTRUMENT OF DELEGATION AND AUTHORISATION

I, Dennis Richardson, Secretary of the Department of Defence pursuant to the *Public Governance, Performance and Accountability Act 2013*, the *Financial Framework (Supplementary Powers) Act 1997* and my appointment under section 61 of the *Judiciary Act 1903*, with effect from 1 July 2015:

- a. **revoke** schedules 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 18A, 19, 20 and 21, being delegations issued under the *Public Governance, Performance and Accountability Act 2013*, *Public Governance, Performance and Accountability Rule 2014*, and the *Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014*; and
- b. **issue** schedules 1, 1A, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 18A, 19, 20, 21 and 21A, being delegations issued under the *Public Governance, Performance and Accountability Act 2013*, *Public Governance, Performance and Accountability Rule 2014*, and the *Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014*;
- c. **revoke** schedules 22 and 24, being authorisations issued under the *Judiciary Act 1903* and the *Financial Management and Accountability (Finance Secretary to Chief Executive of Department of Defence) Delegations 2014-15*; and
- d. **issue** schedules 22 and 24, being authorisations issued under the *Judiciary Act 1903* and the *Financial Management and Accountability (Finance Secretary to Chief Executive of Department of Defence) Delegations 2014-15*; and
- e. **revoke** schedules F7 and 25, being drawing rights issued under section 27 of the *Financial Management and Accountability Act 1997*

to the persons holding, or for the time being occupying or performing the duties of the positions or classes of positions, my powers and functions as specified in the schedules attached to the *Department of Defence Public Governance, Performance and Accountability Delegation*.

In exercising the powers and functions the delegated and authorised officials are to observe the relevant provisions of the applicable legislation, government policy, the Accountable Authority Instructions, other Defence instructions and the directions set out in the Schedules to the attached *Department of Defence Public Governance, Performance and Accountability Delegation*.

Dated this 24<sup>th</sup> day of June 2015

Dennis Richardson, AO  
SECRETARY

---

## Department of Defence

### Public Governance, Performance and Accountability Delegation

#### 1. NAME OF INSTRUMENT

- 1.1 This Instrument is the Department of Defence Public Governance, Performance and Accountability Delegation.

#### 2. ISSUANCE OF NEW DELEGATIONS AND AUTHORISATIONS

- 2.1 With effect from 1 July 2015, the Secretary of Defence has issued the delegations and authorisations under the *Financial Framework (Supplementary Powers) Act 1997*, the *Public Governance, Performance and Accountability Act 2013*, the *Public Governance, Performance and Accountability Rule 2014* and the *Judiciary Act 1903* set out below.

#### 3. DIRECTIONS TO ALL DELEGATES

- 3.1 Where relevant, delegates must comply with the directions issued by the Finance Minister and the Finance Secretary.
- 3.2 A delegate must comply with any directions issued by the Secretary of Defence, including but not limited to any relevant Accountable Authority Instructions.
- 3.3 Delegates must ensure that their decisions are publicly defensible and are an efficient, effective, economical and ethical use of public resources that is not inconsistent with the policies of the Australian Government.
- 3.4 A delegate must avoid situations that could lead to a potential, perceived or real conflict of interest.
- 3.5 Where a limit applies to a delegation, a delegate must not exceed that limit.
- 3.6 Once given authority to act, the delegate's judgement is independent and may be subject to legal or administrative actions. That is, if a delegate is perceived to have made a discriminatory decision, they may be the subject of legal proceedings, and their decisions may also be subject to administrative scrutiny. Therefore, a delegate should always document their decision and the basis of the decision where appropriate, or at least be able to justify their action if required.

#### 4. RECORDING OF DECISIONS

- 4.1 Unless otherwise specified, the delegate must provide their decision in writing (either physically or electronically).
- 4.2 The delegate must record any exercise of a delegation by signing, dating and printing their name and indicating their position title and position number, except where it is not required when exercising the PGPA Act section 23(1) delegation.



- 4.3 For approvals under PGPA Act section 23(3), a document could be a signed brief or minute, an email, an electronic approval within an information system and signed purchase order or purchase order request (see *Acts Interpretation Act 1901*). For minor proposals, such as a taxi fare, a vendor statement/receipt would suffice. A delegate using a credit card may sign on the voucher/receipt provided by the merchant.
- 4.4 Documents recording the exercise of a delegation must be retained and readily accessible for subsequent reference.

## **Table of contents**

### **Part A - Delegations**

#### **Division 1 – Delegations for the commitment of relevant money**

1. Schedule 1 Delegation to approve commitments of relevant money (Commitment Approver)

Part 1: General Proposals for Commitments of Relevant Money (excluding Proposals under Schedule 1 Parts 2 – 6)

Part 2: Exceptions to Part 1 General Proposals for Commitment of Relevant Money

Part 3: Software Purchases (Proposals for Commitment of Relevant Money of Software procurement)

Part 4: ICT Hardware purchases (Proposals for Commitment of Relevant Money for ICT Hardware procurement)

Part 5: Payment to Foreign Forces

Part 6: Proposals for the commitment of relevant money for CASG (excluding proposals relating to corporate ICT software and hardware purchases)

1A. Delegation to grant an indemnity, guarantee or warranty on behalf of the Commonwealth (CASG only)

2. Delegation to enter into, vary and administer an arrangement on behalf of the Commonwealth (PGPA Act Section 23(1) Delegate)

3. Delegation to enter into a grant on behalf of the Commonwealth

#### **Division 2 – Delegations for banking**

4. Delegation to enter into an agreement with a bank .

5. Delegation to open and maintain bank accounts

6. Delegation to enter into a credit card agreement

#### **Division 3 – Delegations for debt management**

7. Delegation to modify the terms and conditions of amounts owing to the Commonwealth

8. Delegation to approve non-recovery of a debt

#### **Division 4 – Delegations for the management of relevant money and property**

9. Delegation to approve agreements or arrangements regarding other CRF money

10. Delegation to approve payment of an amount owed to a person at time of death

11. Delegation to determine liability for the loss of relevant money

12. Delegation to determine liability for the loss of relevant property

13. Delegation to approve gifts of relevant property

14. Delegation to approve the loan or hire of relevant property

15. Delegation to approve the disposal of relevant property

16. Delegation to determine charges for Defence supplied goods and services

17. Delegation to approve quotations for commercial work

18. Delegation to waive charges for Defence Assistance to the Civil Community

- 18A. Delegation to be satisfied that the Consolidated Revenue Fund is appropriated for the repayment

**Division 5 – Delegations under the *Legal Services Directions 2005***

19. Delegation to settle claims by or against the Commonwealth
20. Delegation to approve financial assistance to an official for legal proceedings
21. Delegation to approve payments for the provision of emergency legal services to ADF members overseas

**Division 5A – Other Delegations**

- 21A. Delegation to prescribe certain persons as officials of the Department of Defence

**Part B – Authorisations**

**Division 6 – Authorisation under the *Judiciary Act 1903***

22. Authorisation to bring a suit on behalf of the Commonwealth

**Division 7 – Authorisation under the Constitution**

23. Authorisation to approve Compensation for Detriment caused by Defective Administration

**Division 8 – Authorisation under the *Public Governance, Performance and Accountability Act 2013***

24. PGPA Act section 23(1) authorisation for Special Purpose Aircraft

## DELEGATIONS

### PART A - DELEGATIONS

#### DIVISION 1 – Delegations for the commitment of relevant money

#### SCHEDULE 1 Delegation to approve commitments of relevant money (Commitment Approver)

For Parts 1 to 5 of this Delegation

<b>1</b>	<b>Provision</b>	PGPA Act section 23(3) PGPA Act section 60 PGPA Rule section 18  Schedule 1 part 6 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i>  Determination under the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014: Defence</i> (No. 1 of 2014)
<b>2</b>	<b>Summary of function or power</b>	To approve commitments of relevant money  To grant an indemnity, guarantee or warranty on behalf of the Commonwealth.

#### Part 1: General Proposals for Commitments of Relevant Money (excluding Proposals under Schedule 1 Parts 2 – 6)

Position	Limit of delegation	Note
CDF	Limit of Funds Available	Notes 1 and 7
CFO	Limit of Funds Available	Notes 1, 2 and 7
SES Band 3, O-9 (3 Star)	Limit of Funds Available to Group Budget	Notes 1, 3 and 6
SES Band 2, O-8 ( 2 Star)	Limit of Funds Available to Division Budget	Notes 1 and 6
SES Band 1, O-7 (1 Star)	Limit of Funds Available to Branch Budget	Notes 1 and 6
Group Chief Finance Officer	Limit of Funds Available to Group Budget	Note 6
EL2 and APS equivalent, O-6 (CAPT, COL and GPCAPT)	\$5 million	Note 8
EL1 and APS equivalent, O-5 (CMDR, LTCOL, WGCDR)	\$1 million	Note 8
APS 6 and APS equivalent, O-4 (LCDR, MAJ, SQNLDR)	\$250,000	Note 8
APS 5 and APS equivalent, O-3 (LEUT, CAPT, FLTTLT), WO, WO1, WOFF, WO-N, WOFF-AF	\$80,000	Note 8

**DELEGATIONS**

## FINMAN 2 – Financial Delegations Manual

Position	Limit of delegation	Note
APS 4 and APS equivalent, O-2 (SBLT, LT, FLGOFF), WO2, CPO, FSGT	\$50,000	Note 8
APS 3 and APS equivalent, O-1 (ASLT, 2LT, PLTOFF), SGT, PO	\$10,000	Note 8
Advance Holder	Limit of the Advance	Note 8
LES Business Manager		Notes 4 and 8
LES Defence Office Manager	\$50,000	Note 8
LES Defence Administration Clerk	\$4,000	Note 8
LES Defence Executive Assistant	\$4,000	Note 8
LES Defence Personal Assistant	\$4,000	Note 8
LES – All other LES	\$250	Note 8
LES – All other LES	\$250	Notes 5 and 8
Official includes a contractor whose contract requires them to exercise a delegation and is prescribed as such by a Schedule 21A delegate. The official will be an employee of a contractor where the contractor is not a natural person.	Amount allocated	Notes 5 and 8

**Notes:**

1. Officials at the SES Band 1, 0-7 (1 Star) level and above may approve proposals for the commitment of relevant money for approved business plans with the concurrence of the relevant Group Chief Finance Officer or other designated official.
2. For approval relating to expenditure outside of CFO Group, concurrence must be sought from the Secretary.
3. For the Associate Secretary, the Limit of Funds Available to Group Budget means the Group Budget available for CIOG, Estate and Infrastructure Group (EIG) and DPG.
4. The amount allocated by FASIP.
5. The amount allocated by Defence.
6. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above \$30 million.
7. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above \$50 million.
8. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above the delegate's limit otherwise under this delegation or \$5 million, whichever is the lesser amount.

**Secretary's Directions**

1. The delegate must not approve a proposed commitment of relevant money unless satisfied, after reasonable inquiries, that giving effect to the spending proposal promotes the efficient, effective, economical and ethical use of public resources, that is not inconsistent with the policies of the Australian Government.
2. The delegate must not approve a proposed commitment of relevant money unless satisfied that all required approvals have been obtained.
3. The delegate must ensure that all applicable requirements of the PGPA Act framework are met, including the Commonwealth Procurement Rules (CPRs) and mandatory Defence policy.
4. The delegate must comply with all conditions, including financial limits, attached to his / her delegation.
5. The delegate must ensure that sufficient funds are available to support all payments under the proposed Arrangement.
6. The delegate must make reasonable inquiries, including by consulting appropriate technical specialists to ensure that the delegate is appropriately informed on all relevant matters before exercising the delegation.
7. The delegate must document the advice sought. Where specialist advice has not been sought or is not accepted (in whole or in part), the delegate must document the reasons for his / her decision.
8. Unless specified, no delegate may approve payments to foreign forces.
9. Unless specified, no delegate may approve proposals for the commitment of relevant money ICT software or hardware. Note ICT hardware does not include ICT hardware purchases related to Australian overseas posts, weapons systems or embedded platforms, Urgent Operational Procurement, or High Grade Cryptographic Equipment.
10. The delegate cannot approve a payment to themselves.
11. No delegate may approve a proposed commitment of relevant money relating to grants. Grants may only be approved by the Minister for Defence.
12. The delegate must not approve their own coincidental private expenditure.
13. For procurement of Defence Non Materiel product categories (including all corporate and domestic goods and services, but excluding major capital facilities, software, AMSPA, ICT infrastructure and ICT major projects), where the procurement is valued at more than \$200,000 (including GST), delegates must have regard to any procurement endorsement, and any conditions attached to that endorsement, provided by the Defence Chief Procurement Officer (DCPO), prior to delegates exercising PGPA Act section 23(3) delegation approval. The DCPO procurement endorsement is conducted as part of the Endorsement to Proceed activity undertaken prior to releasing request documentation to the market. DCPO procurement endorsement should also have been sought where a procurement is seeking to establish a standing offer arrangement, and where a contract extension option is being considered, and is available under the contract terms, and where the contract extension is valued at more than \$200,000 (including GST).
14. Where a delegation is approved subject to conditions, a delegate must ensure that those conditions are met before any arrangement is entered into.
15. The delegate must ensure the accurate and timely (within 6 weeks) reporting on AusTender of contracts, agency agreements, standing offers, and amendments to these arrangements, with a value of \$10,000 or above.

**To grant an indemnity, guarantee or warranty on behalf of the Commonwealth**

16. A delegate must not approve a guarantee for the payment of any amount of principle or interest due on a loan
17. A delegate must not approve an indemnity that would meet the costs of civil or criminal penalties of the indemnified party
18. When exercising the delegation, the delegate must consider two overarching policy principles:

- i. the risks are to be born by the party best placed to manage them, and
  - ii. the benefits to the Commonwealth outweigh the risks involved .
- 19. A delegate must not approve an indemnity, guarantee or warranty involving a contingent liability unless satisfied that:
  - i. the likelihood of the event occurring is remote (less than 5% chance), and
  - ii. the most probable expenditure that would need to be made in accordance with the arrangement, if the event occurred, would not be significant (\$30 million)
- 20. Notwithstanding direction 19 above, a delegate may grant an indemnity, guarantee or warranty if:
  - i. it has been explicitly agreed in a decision of Cabinet,
  - ii. it has been explicitly agreed in a decision of the National Security Committee of the Cabinet (NSC) or its successor,
  - iii. it has been explicitly agreed in a decision of the Prime Minister, or
  - iv. it has been approved in writing by the Finance Minister
- 21. In exercising this delegation the delegate must comply with AAI 2.6

**DELEGATIONS****Part 2: Exceptions to Part 1 General Proposals for Commitment of Relevant Money****Delegates**

<b>Position</b>	<b>Limit</b>	<b>Note</b>
ADF Chief Engineer	\$10,000,000	Note 4
ADF Senior Project Engineer	\$5,000,000	Note 4
Financial Adviser (overseas)	\$1,000,000	Note 4
ADF Unit Commanding Officer	\$1,000,000	Note 4
ADF Project Engineer	\$1,000,000	Note 4
ADF SO1/SO2 LOG (Deployed)	\$1,000,000	Note 4
ADF Engineer Works Supervisor	\$500,000	Note 4
ADF Engineer Works Manager	\$1,000,000	Note 4
ADF Unit Quartermaster / Logistics Officer / Maritime Logistics Officer	\$250,000	Note 4
ADF Unit Finance Manager/Officer (APS 4, O-2, WO2, SGT)	\$80,000	Note 4
Cash Office Manager	\$50,000	Note 4
ADF Unit Movements Clerk (ADF/APS)	\$10,000	Note 4
ADF Unit/Sub-unit Admin Clerk (ADF/APS)	\$10,000	Note 4
ADF Unit Operator Supply (CPL, LCPL, equivalent)	\$10,000	Note 4
ADF Unit DUF Clerk (ADF/APS)	\$10,000	Note 4
Transport supervisor, official authorised by a transport supervisor, aircraft captain, Army marine coxswain, vehicle driver, Convoy Commander, Convoy Second-in-Command and Convoy Packet Commander		Notes 1 and 4
Executive Director Strategic Procurement and Contract Support (EIG)	\$350 million	Note 5
Director Procurement and Contracting (EIG)	\$250 million	Note 5
Defence Chief Procurement Officer (NDCPO) (EIG)	\$250 million	Note 5
Director Property Leasing (EIG)	\$20 million	Note 4
Director ACT Office Accommodation (EIG)	\$20 million	Note 4
Director CFI (National, Central West, North East, South East) (EIG)	\$20 million	Note 4
Executive Director CFI (EIG)	\$20 million	Note 4



**DELEGATIONS**

## FINMAN 2 – Financial Delegations Manual

Position	Limit	Note
Regional Director (QLD, CW, SNSW, NNSW, VT) (EIG)	\$10 million	Note 4
Director Business Operations (QLD, CW, SNSW, NNSW, VT) (EIG)	\$10 million	Note 4
Director Customer Support Operations (EIG)	\$10 million	Note 4
Procurement Manager – Complex Procurement (EIG)	\$3 million	Note 4
Senior Procurement Officer – Complex Procurement (EIG)	\$3 million	Note 4
Procurement Officer – Complex Procurement (EIG)	\$3 million	Note 4
Project Director CFI (National, Central West, North East, South East) (EIG)	\$5 million	Note 4
APS 3- Fresh Rations Office Manager-DS-Q (Townsville) (EIG)	\$50,000	Note 4
APS 2- Fresh Rations Ordering Clerk -DS-Q (Townsville) (EIG)	\$50,000	Note 4
APS 3- Fresh Rations Office Manager-DS-Q (Brisbane) (EIG)	\$30,000	Note 4
Financial Adviser (Overseas) (JOC)	Amount Allocated	Notes 2 and 4
SUBOPAETH (JOC)	\$10 million	Notes 3 and 4
DGMAR (JOC)	\$10 million	Note 4
Task Group Commanders (Major (E) or below) (JOC)	\$500,000	Note 4
Task Unit Commanders (Captain (E) or below) (JOC)	\$250,000	Note 4
Task Element Commanders (Captain (E) or below) (JOC)	\$150,000	Note 4

**Notes:**

1. The transaction limit is the limit of funds available for the procurement of fuel, oils and lubricants for the operation or exercise.
2. The amount allocated by JOC through the 'Bulk Fund Certificate' process.
3. Delegation only applies whilst in the capacity of Commander Joint Task Force 627.
4. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above the delegate's limit otherwise under this delegation or \$5 million, whichever is the lesser amount.
5. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above \$30 million.

**Secretary's Directions**

1. Delegates must comply with the Secretary's Directions in Schedule 1 Part 1.

**DELEGATIONS****Part 3: Software Purchases (Proposals for Commitment of Relevant money of Software Procurement)**

This part of the delegation relates to the approval of the commitment of relevant money all software procurement, excluding software purchased as part of weapons systems or embedded platform software or an 'Urgent Operational Procurement'.

<b>Position</b>	<b>Limit of delegation</b>	<b>Note</b>
Associate Secretary	Limit of Funds Available	Note 4
Chief Information Officer (CIOG)	Limit of Funds Available	Note 4
Chief Technology Officer (CIOG)	Limit of Funds Available	Note 4
Deputy Director Capability, Intelligence and Security (ISG)	Limit of Funds Available	Notes 1 and 4
Chief Information Officer (DSTG)	Limit of Funds Available	Notes 2 and 4
Assistant Secretary Group Commercial (CIOG)	\$10,000,000	Note 4
Assistant Secretary Chief Technology Officer, Intelligence and Security (ISG)	\$500,000	Notes 1 and 4
Program Leader, Science Information Services (PLSIS) (DSTG)	\$500,000	Notes 2 and 3
Director, Science Application Services(DSAS) (DSTG)	\$250,000	Notes 2 and 3
Director, Science Client Services(DSCS) (DSTG)	\$250,000	Notes 2 and 3
Director Software (CIOG)	\$5,000,000	Note 3
Software Procurement (DSTG)	\$50,000	Notes 2 and 3

**Notes:**

1. Limited to procurement of software for Intelligence and Security Group.
2. Limited to procurement of software for DSTG research purposes to be installed only on DSTG networks.
3. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above the delegate's limit otherwise under this delegation or \$5 million, whichever is the lesser amount.
4. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above \$30 million.

**Secretary's Directions**

1. Delegates must comply with the Secretary's Directions in Schedule 1 Part 1.

**DELEGATIONS****Part 4: ICT Hardware Purchases (Proposals for Commitment of Relevant Money for ICT Hardware Procurement)**

This part of the delegation relates to the approval of commitment of relevant money for ICT hardware procurement. This does not include ICT hardware procurement at Australian overseas posts, purchases related to weapons systems or embedded platforms, Urgent Operational Procurement, or High Grade Cryptographic Equipment.

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>	<b>Notes</b>
Chief Information Officer (CIOG)	Limit of Funds Available	Note 5
Head ICT Operations Division (CIOG)	Limit of Funds Available	Note 5
Chief Technology Officer (CIOG)	Limit of Funds Available	Note 5
Assistant Secretary Group Commercial (CIOG)	Limit of Funds Available	Note 5
Director Hardware (CIOG)	\$2,000,000	Note 4
Assistant Director Hardware (multiple positions) (CIOG)	\$500,000	Note 4
Chief Information Officer (DSTG)	Limit of Funds Available	Notes 2 and 5
Chief Information Officer (DSTG)	Limit of Funds Available	Notes 2 and 5
Program Leader, Science Information Services (PLSIS) (DSTG)	\$500,000	Notes 2 and 4
Director, Research Network & Infrastructure Services (DRNIS) (DSTG)	\$250,000	Notes 2 and 4
Director, Science Client Services (DSTG)	\$250,000	Notes 2 and 4
Hardware Procurement (DSTG)	\$50,000	Notes 2 and 4
Deputy Director Capability (ISG)	Limit of Funds Available	Notes 3 and 5
Assistant Secretary Chief Technology Officer (ISG)	Limit of Funds Available	Notes 3 and 5
Assistant Secretary Capability Provision (ISG)	Limit of Funds Available	Notes 3 and 5
Assistant Secretary Capability Assurance (ISG)	Limit of Funds Available	Notes 3 and 5
Director of Chief Technology Officer Resources (ISG)	\$500,000	Notes 3 and 4
Director of Capability Assurance Infrastructure Services (ISG)	\$500,000	Notes 3 and 4
Director of Capability Provision Business Management (ISG)	\$500,000	Notes 3 and 4

**Notes**

1. Limited to authorising the procurement of ICT hardware of the type and specification approved for use on CIOG managed networks.
2. Limited to the procurement of ICT hardware for DSTG Research Networks. The DSTG is required to notify the CIOG prior to procurement.

**DELEGATIONS**

3. Limited to the procurement of ICT hardware for Intelligence Networks under the care, custody and control of the Intelligence and Security Group including the Defence Top Secret Network.
4. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above the delegate's limit otherwise under this delegation or \$5 million, whichever is the lesser amount.
5. For proposals for the commitment of relevant money that contain or consist of an indemnity, guarantee or warranty ('contingent liability'), the delegate may only authorise the contingent liability if the most probable expenditure that could arise from the contingent liability if the contingent liability should crystallise, would not be above \$30 million.

**Secretary's Directions**

Delegates must comply with the Secretary's Directions in Schedule 1 Part 1.

**Part 5: Payment to Foreign Forces**

This part of the delegation allows delegates, at their discretion, to make payments to Foreign Forces. Such payments must be for the purpose of a scheme which has been approved by CJOPS as an efficient, effective, economical and ethical use of resources.

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>	<b>Notes</b>
DCJOPS	\$5,000	
Task Force Commander (JOC)	\$1,000	Note 1
Task Group Commanders (JOC)	\$500	Note 2
Task Unit Commander (JOC)	\$200	Note 3
Financial Adviser (JOC)	\$200	Note 4

**Notes**

1. **Task Force Commander** is defined as the member appointed by CJOPS to the position designated in the CJOPS approved Operational Manning Document as the Task Force Commander.
2. **Task Group Commander** is defined as the member appointed to the position designated in the CJOPS approved Operational Manning Document as a Task Group Commander.
3. **Task Unit Commander** is defined as the member appointed to the position designated in the CJOPS approved Operational Manning Document as a Task Unit Commander.
4. **Financial Adviser (JOC)** is defined as a Financial Adviser in a CJOPS approved Operational Manning Document.

**Part 6: Proposals for commitment of relevant money for CASG (excluding proposals relating to corporate ICT software and hardware purchases)**

This part of the delegation relates to the approval of commitments of relevant money for Capability Acquisition and Sustainment Group (CASG)

<b>1</b>	<b>Provision</b>	PGPA Act section 23(3) PGPA Rule section 18 Schedule 1 part 6 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i>
<b>2</b>	<b>Summary of function or power</b>	To approve commitments of relevant money (This delegation does not include the power to approve an indemnity, guarantee or warranty on behalf of the Commonwealth.)

**CASG Delegates**

<b>Position</b>	<b>Limit of delegation</b>	<b>Note</b>
SES Band 1, O-7 (1 Star) to SES Band 3 / O-9 (3 Star) (CASG)	Limit of Funds Available within relevant budget	
EL2, O-6 (COL(E)) holding a position of SPO Director, Project Director, Program Director or equivalent (CASG)	\$20,000,000	Note 1
EL 2, O-6 (COL(E)) (CASG)	\$5,000,000	Note 1
EL 1, O-5 (LTCOL(E)) holding a position of Project Manager, Program Manager, Sustainment Manager or equivalent (CASG)	\$10,000,000	Note 1
EL 1, O-5 (LTCOL(E)) (CASG)	\$3,000,000	Note 1
APS 5, CAPT (E) to APS 6, MAJ(E) (CASG)	\$1,000,000	Note 1
APS 2, CPL (E) to APS4, LT(E) (CASG)	\$500,000	Note 1
APS 1, PTE (E) (CASG)	\$10,000	Note 1
Official (other than CASG) APS 1, PTE (E) to SES Band 2, O-8 (2 Star)	Refer Note	Note 2
CASG Locally Engaged Employee (staff)	\$1,000,000	Note 3
DFAT Head of Mission	Refer Note 3	Note 3
DFAT Finance Manager (overseas)	Refer Note 3	Note 3

**DELEGATIONS**

Position	Limit of delegation	Note
Official (a contractor whose contract requires them to exercise a delegation, and as approved by an SES or equivalent level) the official will be an employee of the contractor where the contractor is not a natural person.	Amount Allocated	Note 2
Director General Land Support Systems (EL2.2) (Position Number 572329)	Limit of Funds Available within relevant budget	Note 4

**Notes:**

1. Not exceeding the limit of funds available within the relevant budget
2. The amount allocated by CASG for the proposed arrangement being considered, but not exceeding the limit of delegation for a CASG official of the same rank.
3. Up to the amount allocated to the post for CASG purposes, or, the amount allocated by CASG for the proposed arrangement being considered.
4. [May approve official travel as SES Band 1, O-7 \(1 star\).](#)

**Secretary's Directions**

1. The delegate must not approve a proposal for the commitment of relevant money unless satisfied, after reasonable inquiries, that giving effect to the spending proposal promotes the efficient, effective, economical and ethical use of public resources, that is not inconsistent with the policies of the Australian Government.
2. The delegate must ensure that all applicable requirements of the PGPA Act framework are met, including the Commonwealth Procurement Rules (CPRs) and mandatory Defence policy (including the DPPM and DMI (Procs).
3. The delegate must not approve a proposed commitment of relevant money unless satisfied that all required approvals have been obtained.
4. The delegate must comply with all conditions, including financial limits, attached to his / her delegation.
5. The delegate must not approve a proposed commitment of relevant money for Complex procurements unless and Endorsement to Proceed has been obtained.
6. If the proposed commitment of relevant money involves a contingent liability, the delegate must not approve the proposal unless the contingent liability has been approved by a contingent liability delegate in Schedule 1A.
7. The delegate must ensure that sufficient funds are available to support all payments under the proposed Arrangement.
8. The delegate must make reasonable inquiries, including by consulting appropriate technical specialists to ensure that the delegate is appropriately informed on all relevant matters before exercising the delegation.
9. The delegate must document the advice sought. Where specialist advice has not been sought or is not accepted (in whole or in part), the delegate must document the reasons for his / her decision.
10. Unless specified, no delegate may approve payments to foreign forces.
11. Unless specified, no delegate may approve proposals for the commitment of relevant money for ICT software or hardware. Note ICT hardware does not include ICT hardware purchases related to Australian overseas posts, weapons systems or embedded platforms, Urgent Operational Procurement, or High Grade Cryptographic Equipment.

12. The delegate cannot approve a payment to themselves.
13. No delegate may approve a proposal for the commitment of relevant money relating to grants. Grants may only be approved by the Minister for Defence.
14. The delegate must not approve their own coincidental private expenditure.
15. Where a delegation is approved subject to conditions, a delegate must ensure that those conditions are met before any arrangement is entered into.
16. The delegate must ensure the accurate and timely (within 6 weeks) reporting on AusTender of contracts, agency agreements, standing offers, and amendments to these arrangements, with a value of \$10,000 or above.



**DELEGATIONS****SCHEDULE 1A Delegation to grant an indemnity, guarantee or warranty on behalf of the Commonwealth (CASG only)**

<b>1</b>	<b>Provision</b>	PGPA Act section 60  Schedule 1 part 6 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i>  Determination under the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014: Defence (No. 1 of 2014)</i>
<b>2</b>	<b>Summary of function or power</b>	To grant an indemnity, guarantee or warranty on behalf of the Commonwealth

1. Section 60 of the PGPA Act provides the Finance Minister the power to grant an indemnity, guarantee, warranty or other contingent liability on behalf of the Commonwealth. The Finance Minister has delegated this power to the Secretary with limits. In addition the Finance Minister has issued a Defence Determination further expanding the limits of his delegation. The Secretary further delegates this power to Defence officials through this Delegation Schedule.

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>
CASG SES Band 1, O-7 (1 Star) to SES Band 3, O-9 (3 Star)	\$50 million
Official (a contractor whose contract requires them to exercise a delegation to grant a contingent liability, and as approved by an SES or equivalent level) the official will be an employee of the contractor where the contractor is not a natural person.	Amount allocated

**Secretary's Directions****To grant an indemnity, guarantee or warranty on behalf of the Commonwealth**

1. A delegate must not approve a guarantee for the payment of any amount of principle or interest due on a loan
2. A delegate must not approve an indemnity that would meet the costs of civil or criminal penalties of the indemnified party
3. When exercising the delegation, the delegate must consider two overarching policy principles:
  - i. the risks are to be born by the party best placed to manage them, and
  - ii. the benefits to the Commonwealth outweigh the risks involved .
4. A delegate must not approve an indemnity, guarantee or warranty involving a contingent liability unless satisfied that:
  - i. the likelihood of the event occurring is remote (less than 5% chance), and
  - ii. the most probable expenditure that would need to be made in accordance with the arrangement, if the event occurred, would not be significant (\$50 million)

## **DELEGATIONS**

5. Notwithstanding direction 4 above, a delegate may grant an indemnity, guarantee or warranty if:
  - i.it has been explicitly agreed in a decision of Cabinet,
  - ii.it has been explicitly agreed in a decision of the National Security Committee of the Cabinet (NSC) or its successor,
  - iii.it has been explicitly agreed in a decision of the Prime Minister, or
  - iv.it has been approved in writing by the Finance Minister
6. In exercising this delegation the delegate must comply with AAI 2.6

## **SCHEDULE 2      Delegation to enter into, vary and administer arrangements on behalf of the Commonwealth (PGPA Act Section 23(1) Delegate)**

<b>1</b>	<b>Provision</b>	PGPA Act section 23(1)
<b>2</b>	<b>Summary of function or power</b>	To enter into, vary and administer arrangements on behalf of the Commonwealth

### **Delegates**

<b>Position</b>	<b>Limit of delegation</b>
All Officials	Unlimited

#### **Notes:**

1. 'Arrangement' includes a contract, agreement, deed, understanding or purchase order.
2. Arrangements may be in writing or in electronic form. They must be readily accessible so as to be usable for subsequent reference.
3. An oral contract through a simple procurement process and involving the use of a Commonwealth Credit Card (such as hire of a taxi, payment for excess baggage, etc) does not have to be separately recorded in writing.
4. An officer, instructor or cadet in the Australian Air Force Cadets, the Australian Army Cadets or the Australian Navy Cadets is not an official for the purpose of this delegation.
5. For CASG Arrangements - If the proposed arrangement does not involve the commitment of relevant money (and therefore does not require a Section 23 Commitment Approval delegation to be exercised) you must:
  - have a rank of EL 2/ o-6 (COL(E)) or above, and
  - be satisfied that the proposed arrangement represents proper use and management of public resources and is not inconsistent with the policies of the Australian Government.
6. 'Official' includes a contractor whose contract requires them to exercise a delegation and is prescribed as such by a Schedule 21A delegate. The official will be an employee of a contractor where the contractor is not a natural person.

### **Secretary's Directions.**

1. The delegate must not enter into an arrangement that commits relevant money unless it has been approved by a section 23(3) commitment approval delegate.
2. The delegate must not enter into an arrangement that commits relevant money if the value of the arrangement exceeds that amount approved by the Section 23 (3) commitment approval delegate.
3. The acquisition by agreement of an interest in land or of a leasehold interest in land must be approved by Defence officials who have been issued a delegation under the *Lands Acquisition Delegation 2012*.
4. Agreements for custody of money or banking agreements must first be approved under FINMAN 2 schedules 4 or 9.

**SCHEDULE 3      Delegation to enter into a grant on behalf of the Commonwealth**

<b>1</b>	<b>Provision</b>	<i>Financial Framework (Supplementary Powers) Act 1997</i> section 32B
<b>2</b>	<b>Summary of function or power</b>	To enter into a grant on behalf of the Commonwealth

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>
All Officials	Unlimited

**Secretary's Directions**

1. The delegate must not enter into a grant unless the Minister for Defence has approved the grant under PGPA Act section 71 in writing.
2. The delegate must ensure the accurate and timely (no later than fourteen working days) reporting of grants on the Defence website.

## DELEGATIONS

### FINMAN 2 – Financial Delegations Manual

---

## DIVISION 2 – Delegations for banking

### SCHEDULE 4 Delegation to enter into an agreement with a bank

1	<b>Provision</b>	Schedule 1 part 1 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i> (PGPA Act section 53)
2	<b>Summary of function or power</b>	To enter into agreements with any bank for the receipt, custody, payment or transmission of relevant money

#### Delegates

Position	Limit
CFO	Unlimited
FASRA (CFOG)	Unlimited

#### Secretary's Directions

1. The delegate must comply with the Finance Minister's directions.
2. Any agreement entered into for an encashment facility must require that cheques be counter signed where it exceeds \$10,000 in value.

## DELEGATIONS

### FINMAN 2 – Financial Delegations Manual

#### SCHEDULE 5 Delegation to open and maintain bank accounts

<b>1</b>	<b>Provision</b>	Schedule 1 part 1 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i> (PGPA Act section 53)
<b>2</b>	<b>Summary of function or power</b>	To open and maintain official bank accounts in accordance with an agreement established by a FINMAN 2 schedule 4 delegate

#### Delegates

Position	Limit of delegation
CFO	Unlimited
FASRA (CFOG)	Unlimited
ASFS (CFOG)	Unlimited

#### Secretary's Directions

1. The delegate must comply with the Finance Minister's directions.
2. The delegate may grant access to bank accounts established under this delegation and may determine the conditions and limits under which such access is to be allowed.

## DELEGATIONS

### SCHEDULE 6 Delegation to enter into a credit card agreement

1	Provision	Schedule 1 part 4 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i>  (PGPA Act section 56)
2	Summary of function or power	On behalf of the Commonwealth, to enter into agreements under the Act, for borrowing money, by obtaining credit by way of credit card or credit voucher

#### Delegates

Position	Limit of delegation
CFO	Unlimited
FASRA (CFOG)	Unlimited

#### Finance Minister's Directions

##### Only for issue and use of credit cards and credit vouchers

1. The delegate is permitted to enter into agreements only for the issue to, and use by, the Commonwealth of credit cards or credit vouchers.

**Note:** Subsection 56(3) provides that the agreement must require the amount borrowed to be repaid by the Commonwealth within 90 days and it must be in accordance with any requirement prescribed by the rules.

## DELEGATIONS

### DIVISION 3 – Delegations for debt management

#### SCHEDULE 7 Delegation to modify the terms and conditions of amounts owing to the Commonwealth

<b>1</b>	<b>Provision</b>	Schedule 1 part 9 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i> (PGPA Act section 63)
<b>2</b>	<b>Summary of function or power</b>	To allow payment by instalments, or defer the time for payment of an amount owing to the Commonwealth

#### Delegates

Position	Limit	Note
CDF	Unlimited	
CFO	Unlimited	
Associate Secretary	\$300,000	Notes 7, 8 and 9
First Assistant Secretary Resource and Assurance (CFOG)	\$300,000	Notes 7, 8 and 9
Assistant Secretary Financial Services (CFOG)	\$200,000	Notes 7, 8 and 9
Inspector General (OSCDF)	\$200,000	Note 7
Deputy Secretary Estate and Infrastructure (EIG)	\$200,000	Notes 4, 5 and 6
First Assistant Secretary Governance and Reform Division	\$200,000	Notes 4, 5 and 6
Director General People Services (DPG)	\$200,000	Note 8
Assistant Secretary Legal Services (DL)	\$200,000	Notes 8 and 9
General Counsel CASG	\$200,000	Notes 2 and 3
Deputy General Counsel CASG (Position No 572306)	\$100,000	Notes 2 and 3
Director Litigation (DL)	\$50,000	Notes 2 and 3
Director Finance Business Centre (CFOG)	\$50,000	Note 9
Director PAC Melbourne (DPG)	\$50,000	Note 8
Manager DEFPAC (DPG)	\$40,000	Note 8
Manager Civilian PAC (DPG)	\$40,000	Note 8
Manager Specialist Personnel Administration, PAC-Melbourne (DPG)	\$40,000	Note 8
Complex Case Manager, PAC-Melbourne (DPG)	\$25,000	Note 8
Manager Payroll Recovery, PAC-Melbourne (DPG)	\$25,000	Note 8
Assistant Director Finance Business Centre (CFOG)	\$25,000	Note 9
DIR (IG) (OSCDF)	\$20,000	Note 7
PAC Operations Manager , SPA, PAC-Melbourne (DPG)	\$15,000	Note 2
Manager General Pay, PAC-Melbourne (DPG)	\$15,000	Note 8
Manager Special Pay, PAC-Melbourne (DPG)	\$15,000	Note 8



**DELEGATIONS**

## FINMAN 2 – Financial Delegations Manual

Manager Business Support, PACs both civilian and military (DPG)	\$15,000	Note 8
Director MPAC (DPG)	\$15,000	Note 2
Director MPAC – Defence Support (DPG)	\$15,000	Note 8
AR Collections Manager (NDARC) (CFOG)	\$5,000	Note 9
AR Collections Team Leader (NDARC) (CFOG)	\$5,000	Note 9
Senior Recovery Officer, PAC-Melbourne (DPG)	\$2,000	Note 8
Manager Reserve Pay Accounting Centre (DPG)	\$2,000	Note 8
Assistant Director MPAC (Operations) (DPG)	\$2,000	Note 8
Assistant Director MPAC (Business Support)(DPG)	\$2,000	Note 8
MPAC Manager (DPG)	\$2,000	Note 8
MPAC Team Leader (DPG)	\$2,000	Note 8
ADF CO MPAC(DPG)	\$2,000	Note 8
ADF XO MPAC (DPG)	\$2,000	Note 8

**Notes**

1. To allow payment by instalments of fraud related debts only.
2. To allow payment by instalments of salaries and allowances, and related debts only.
3. To allow payment by instalments of ROMAN related debts only.
4. To defer the time for payment of fraud related debts only.
5. To defer the time for payment of salaries and allowances, and related debts only.
6. To defer the time for payment of ROMAN related debts only.
7. To allow payment by instalments or to defer the time for payment of fraud related debts only.
8. To allow payment by instalments or to defer the time for payment of salaries and allowances, and related debts only.
9. To allow payment by instalments or to defer the time for payment of ROMAN related debts only.

**Finance Minister's Directions****1 Generally amounts owing to the Commonwealth are to be paid in full**

- (1) The delegate must have regard to the basic principle that, unless otherwise allowed by law (for example, under statute or contract), amounts owing to the Commonwealth should be paid in full immediately they become due.
- (2) In a situation where it is not possible or reasonable for an amount to be paid in full immediately and in the absence of any statutory right of the debtor to do otherwise, consideration may be given to contracting with the debtor to allow payment of the amount by instalments or in full at a deferred date.

**2 Scope of delegation**

The delegate may only modify the terms and conditions to:

- (a) defer the time for payment of an amount owing to the Commonwealth; and

- (b) allow payment by instalments of an amount owing to the Commonwealth.

### **3 Specific requirements**

- (1) The delegate must comply with the following directions.

#### *Cases of hardship*

- (2) In a situation of claimed hardship, the delegate must:
  - (a) require the debtor to provide evidence (by a statutory declaration or other means) sufficient to satisfy the delegate that it would be unreasonable to require the debtor to discharge the debt otherwise than at a deferred date; and
  - (b) have regard to the Commonwealth's interests not being subordinate to other creditors of the same ranking.

#### *Instalments*

- (3) When allowing *payment by instalments*, the delegate must impose conditions on such payment with the object of ensuring that the Commonwealth recovers the amount as soon as is reasonably practicable, having regard to the debtor's ability to repay.

#### *Interest*

- (4) The delegate must:
  - (a) ordinarily impose interest at the 90 day bank-accepted bill rate (available from the Reserve Bank of Australia); and
  - (b) not impose interest at a higher rate than the 90 day bank-accepted bill rate; and
  - (c) if a lesser rate of interest, or no interest, is imposed - record in writing the reasons for doing so.

*Note 1:* A reason for not imposing interest, or imposing less than the specified rate, is that, in the particular case, the imposition of interest would cause undue financial hardship.

*Note 2:* This direction does not apply to Court-awarded judgment debts, as provision for interest will usually be made in the laws of the State or Territory in which judgment was obtained.

#### *Information to be given to debtor*

- (5) If the delegate decides to modify the terms and conditions, of an amount owing to the Commonwealth:
  - (a) the debtor must be informed in writing of the following matters:
    - (i) the amount owing to the Commonwealth;
    - (ii) the date or dates when payment is due;
    - (iii) the interest rate (if any);
    - (iv) any other matter the delegate considers relevant, taking into account the evidence of hardship;
    - (v) the conditions of acceptance specified in subdivision 4; and
  - (b) the debtor must confirm, in writing, acceptance of the matters specified above.

*Note:* If the debtor does not confirm, in writing, acceptance of the conditions specified then the amounts owing to the Commonwealth should be paid in full when they become due.

### **4 Conditions**

The conditions of acceptance of payment of a debt by instalments or at a deferred date are as follows:

**DELEGATIONS**

- (a) the delegate may, at any time, review and, if necessary, revise the arrangements to determine whether different conditions should be imposed, taking into account the debtor's ability to pay; and
- (b) if the debtor is an official, upon termination of employment, or other engagement, with the Commonwealth, the amount outstanding must be set off against any final moneys due; and
- (c) any default of the conditions may result in legal action being commenced to recover the amount owing; and
- (d) if legal action is commenced, the Commonwealth may seek to recover its costs from the debtor.

## DELEGATIONS

### SCHEDULE 8 Delegation to approve non-recovery of a debt

1	<b>Provision</b>	PGPA Act section 103© and 110 PGPA Rule section 11
2	<b>Summary of function or power</b>	To approve non-recovery of a debt owed to the Commonwealth

#### Delegates

Position	Limit	Note
CDF	Unlimited	
CFO	Unlimited	
FASRA (CFOG)	\$200,000	
Assistant Secretary Financial Services (CFOG)	\$50,000	Notes 1 and 4
IG (OSCDF)	\$50,000	Notes 1 and 3
Deputy Secretary Estate and Infrastructure (EIG)	\$50,000	Note 1
First Assistant Secretary Governance and Reform	\$50,000	Note 1
Director General People Services (DPG)	\$50,000	Notes 1 and 2
DIR(IG)	\$10,000	Notes 1 and 3

#### Notes:

- For paragraph 1 (b) and (c) of the Secretary's Directions, the delegate can approve the non-recovery of a debt up to the financial limit listed in the Column 'Limit'. However, for paragraph (a) the delegate can approve the non-recovery of a debt up to \$150 only.
- For Salaries and Allowances, and related debts only.
- For fraud related debts only.
- For ROMAN related debts only.

#### Secretary's Directions

- The delegate may determine that recovery of a debt is not to be pursued on the grounds that:
  - the delegate considers that it is not economical to pursue recovery of the debt;
  - the delegate is satisfied that the debt is not legally recoverable; or
  - the debt has been written off as authorised by an Act.
- The delegate must not approve the waiver of an amount owing to the Commonwealth.
- The delegate must understand and comply with any relevant instructions detailed in AAI 9 – Managing Debt, and any other relevant AAI.
- An amount owing to the Commonwealth includes an amount that is owing but not yet due for payment.

## DELEGATIONS

### DIVISION 4 – Delegations for the management of relevant money and property

#### SCHEDULE 9 Delegation to approve agreements or arrangements regarding other CRF money

<b>1</b>	<b>Provision</b>	PGPA Rule section 29
<b>2</b>	<b>Summary of function or power</b>	To approve agreements or arrangements regarding other CRF money

#### Delegates

<b>Position</b>	<b>Limit of delegation</b>
CDF	Unlimited
CFO	Unlimited
FASRA (CFOG)	Unlimited
SES Band 3, O-9 (3 Star)	Note 1
Group Chief Finance Officer	Note 1
HDSO (EIG)	Note 1

#### Note:

1. Agreements or arrangements only for the receipt and custody of other CRF money.

#### Secretary's Directions

1. The delegate must ensure that any arrangement entered into relating to the receipt, custody or expenditure of other CRF money complies with section 2 of this schedule.
2. The arrangement must:
  - (a) promote the efficient, effective, economical and ethical use and management of the other CRF money that is not inconsistent with the policies of the Australian Government; and
  - (b) be in writing; and
  - (c) require the other CRF money to be deposited in a bank account as soon as is practicable; and
  - (d) require the other party to the arrangement:
    - (i) to cause records to be kept that properly record and explain the receipt, custody and expenditure of the other CRF money; and
    - (ii) to allow those records to be conveniently and properly audited; and
  - (e) require any interest earned on the other CRF money to be remitted in full to the Commonwealth (including a requirement about the timing and frequency of remitting such interest); and
  - (f) include a requirement about the timing and frequency of any remittance of the other CRF money to the Commonwealth required under the arrangement; and
  - (g) include a requirement about the timing and frequency of any payments of other CRF money to another person required under the arrangement.

## DELEGATIONS

### SCHEDULE 10 Delegation to approve payment of an amount owed to a person at time of death

<b>1</b>	<b>Provision</b>	Schedule 2 part 1 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i> (PGPA Rule section 25)
<b>2</b>	<b>Summary of function or power</b>	To authorise the payment of an amount owed to a person at the time of their death to the person who the delegate considers should receive the payment

#### Delegates

Position	Limit of delegation
CDF	Unlimited
SES Band 3, O-9 (3 Star)	Unlimited
SES Band 2, O-8 (2 Star)	Unlimited
COMASC (O-7 or lower)	Unlimited
Group Chief Finance Officer	Unlimited
DGPS (DPG)	Unlimited
DG DCO (DPG)	Unlimited
Director PAC-M(DPG)	Unlimited
DPMPP (DPG)	Unlimited

#### Secretary's Directions

1. The delegate may authorise the payment without requiring production of probate of the will of the deceased person or letters of administration of the estate of the deceased person.
2. The delegate must have regard to the persons who are entitled to the property of the deceased person under the deceased person's will or under the law relating to the disposition of the property of deceased persons. Where a decision cannot be made as to the rightful recipient, advice must be sought from Defence Legal.

**DELEGATIONS****SCHEDULE 11 Delegation to determine liability for the loss of relevant money**

<b>1</b>	<b>Provision</b>	PGPA Act sections 68 and 69
<b>2</b>	<b>Summary of function or power</b>	To determine whether an official is liable to pay the Commonwealth an amount equal to a loss of relevant money in the official's custody

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>
CDF	Unlimited
CFO	Unlimited
FASRA	\$200,000
IG	\$200,000
SES Band 3, O-9 (3 Star)	\$50,000
SES Band 2, O-8 (2 Star)	\$30,000
SES Band 1, O-7 (1 Star)	\$20,000
COMASC (O-6 or lower)	\$20,000
DIR (IG)	\$20,000
Group Chief Finance Officer	\$20,000
Regional Director Defence Support (EIG)	\$10,000
DCOORD HQJOC	\$10,000
DFIN HQJOC	\$10,000
Financial Advisor (Overseas)	\$10,000
ADF Unit Commanding Officer	\$5,000

**Secretary's Directions**

1. The delegate must determine a course of action relating to a report of a loss of relevant money and determine the liability of any official in relation to the loss.
2. The delegate may appoint an official or other person to investigate a loss of relevant money, or seek a report from an official or other person. Upon receiving a report the delegate must decide on one of the following courses of action:
  - (a) that an official is liable and the amount of the loss should be pursued in full as a debt owing to the Commonwealth;
  - (b) that the amount of the loss should be reduced on the grounds that the person otherwise liable is liable to pay only so much of the amount of the loss as is just and equitable having regard to the person's share of the responsibility for the loss, and that this reduced amount should be pursued as a debt owing to the Commonwealth;
  - (c) that the amount of the loss should not be pursued on the grounds that it is not legally recoverable;
  - (d) that the amount of the loss should not be pursued on the grounds that no official caused or contributed to the loss by misconduct, or by a deliberate or serious disregard of reasonable standards of care;
  - (e) that the amount of the loss should not be pursued on the grounds that the nominal custodian took reasonable steps in all the circumstances to prevent the loss; or
  - (f) that an official is prima facie liable but the amount of the loss should not be pursued on the grounds that it is not economical to pursue.

## DELEGATIONS

### FINMAN 2 – *Financial Delegations Manual*

---

3. The delegate must investigate any loss where fraud, theft or misappropriation is suspected in accordance with DI(G) ADMIN 45-2, *Reporting and Management of Notifiable Incidents*, and/or DI(G) FIN 12-1, *The Control of Fraud in Defence and the Recovery of Public Monies*, as appropriate.



**DELEGATIONS****SCHEDULE 12 Delegation to determine liability for the loss of relevant property**

<b>1</b>	<b>Provision</b>	PGPA Act sections 68 and 69
<b>2</b>	<b>Summary of function or power</b>	To determine whether an official is liable to pay the Commonwealth an amount equal to the value of relevant property lost or damaged while in the official's custody

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>
CDF	Unlimited
SES Band 3, O-9 (3 Star)	Unlimited
SES Band 2, O-8 (2 Star)	\$5,000,000
DGSC (VCDFG-JLC)	\$1,000,000
DSCS (VCDFG-JLC)	\$750,000
SES Band 1, O-7 (1 Star)	\$500,000
COMASC (O-6 or lower)	\$500,000
Group Chief Finance Officer	\$500,000
COMD DNSDC (VCDFG-JLC)	\$500,000
COMD JLU (V) (VCDFG-JLC)	\$500,000
DEOS (VCDFG-JLC)	\$500,000
JLC Unit Commanding Officer (VCDFG-JLC)	\$250,000
COFS/CSO Support (O-6)	\$200,000
Financial Adviser (overseas)	\$200,000
EL2, O-6	\$200,000
COMDT (O-6)	\$200,000
EL1, O-5	\$100,000
ADF Unit Commanding Officer	\$100,000
DDEOSD (VCDFG-JLC)	\$100,000
Logistics Manager / OIC Logistics Operations ADF	\$100,000
Regional Director Defence Support (EIG)	\$100,000
ADF Unit Second in Command	\$50,000
ADF Unit Quartermaster/Maritime Logistics Officer/Logistics Officer	\$50,000
Contract Manager / Contract Services Manager (VCDFG-JLC)	\$50,000
Warehousing and Distribution Officer (APS 5)	\$50,000
Fleet Manager / Fleet Services Manager	\$50,000
Contract Manager AAVNTC	\$20,000
Stock Control Officer (VCDFG-JLC)	\$10,000
OPSO MP COY, 1 MP BN	\$5,000
WO CO-ORD SME	\$5,000
ADF Unit RQMS/SNCO Supply (SNCO SUP)	\$5,000

**Secretary's Directions**

1. The delegate must determine a course of action relating to a report of a loss of or damage to relevant property and determine the liability of any official in relation to the loss.

**DELEGATIONS**

2. The delegate must comply with any relevant instructions detailed in any other relevant AAI, and other instructions, policies and procedures issued from time to time relating to the loss of or damage to relevant property.
3. The delegate may appoint an official or other person to investigate a loss of or damage to relevant property, or seek a report from an official or other person. Upon receiving a report the delegate must decide on one of the following courses of action:
  - (a) that an official is liable and the amount of the loss should be pursued in full;
  - (b) that the amount of the loss should be reduced on the grounds that the person otherwise liable is liable to pay only so much of the amount of the loss as is just and equitable having regard to the person's share of the responsibility for the loss or damage, and that this reduced amount should be pursued;
  - (c) that the amount of the loss should not be pursued on the grounds that it is not legally recoverable;
  - (d) that the amount of the loss should not be pursued on the grounds that no official caused or contributed to the loss by misconduct, or by a deliberate or serious disregard of reasonable standards of care;
  - (e) that the amount of the loss should not be pursued on the grounds that the nominal custodian took reasonable steps in all the circumstances to prevent the loss;
  - (f) that an official is prima facie liable but the amount of the loss should not be pursued on the grounds that it is not economical to pursue; or
  - (g) other action in accordance with the relevant AAI, where the relevant property is in the custody of a contractor or other outsider, notwithstanding any action taken against an official in accordance with any of sub-paragraphs a. to f. above.
4. The delegate must investigate or arrange for the investigation of the following losses:
  - (a) attractive or sensitive items, such as weapons and associated controlled repair parts, classified equipment, controlled medical supplies, etc, irrespective of value;
  - (b) any items where fraud, theft or misappropriation is suspected; and
  - (c) any other items valued over \$1,000 (the delegate may at their discretion investigate other items under \$1,000).
5. The amount of the loss is:
  - (a) where a damaged item is to be repaired – the less of (i) the cost of repairing the item, or (ii) the value of the item at the end of the month prior to the damage occurring; or
  - (b) in any other case – the value of the item at the end of the month prior to the loss or damage.
6. The delegate must calculate the value of the property in accordance with the relevant AAI.
7. The delegate must investigate any loss where fraud, theft or misappropriation is suspected in accordance with DI(G) ADMIN 45-2, *The reporting and management of notifiable incidents*, and/or DI(G) FIN 12-1, *The Control of Fraud in Defence*, as appropriate.
8. The delegate must ensure that the Defence accounting record is adjusted for an item which is lost, or is damaged and is not to be repaired and returned, to reflect the loss.

## DELEGATIONS

### FINMAN 2 – Financial Delegations Manual

## SCHEDULE 13 Delegation to approve gifts of relevant property

<b>1</b>	<b>Provision</b>	Schedule 1 part 10 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i> (PGPA Act section 66)
<b>2</b>	<b>Summary of function or power</b>	To authorise a gift of relevant property

### Delegates

Position	Limit of delegation	Note
CDF	Unlimited	
SES Band 3, O-9 (3 Star)	\$500,000	
DCJOPS	\$500,000	
CJLOG (VCDFG – JLC)	\$500,000	
COMASC	\$500,000	Note 1
CJHLTH (VCDFG-JHC)	\$100,000	
FASIP	\$100,000	Note 2
FASICTRD (CIOG)	\$100,000	Note 3
Group Chief Finance Officer	\$100,000	
Regional Director Defence Support (EIG)	\$10,000	Note 4
COFS/CSO Support (O-6, O-5)	\$10,000	Note 4
ADF Unit Commanding Officer	\$10,000	Note 4
ADF Unit Second in Command	\$5,000	Note 4

### Notes:

- For relevant property used in overseas/UN operations.
- For Defence Cooperation Program and other overseas purposes.
- For ICT equipment.
- For property that is obsolete or surplus to requirements, such as cooking and messing equipment, clothing, bedding, tentage and furniture. This disposal is to be for charitable or civil emergency purposes only and offering the property to Emergency Management Australia should be considered before entering into any other arrangement.

### Finance Minister's Directions

#### 1 No authorising the gifting of military firearms

A delegate must not authorise a gift of military firearms.

#### 2 Overarching principles

- When contemplating whether to authorise a gift of relevant property, a delegate must consider the overarching principles that, if appropriate to do so, the relevant property should be:
  - agreed to be transferred with or without payment to another government entity within Australia (including State or Territory governments); or
  - sold at market value, where it is economical to do so.
- A departure from the Commonwealth's overarching principles, encompassing disposal by gift, is permitted if the relevant property in question is:
  - genuinely surplus to the entity's requirements; and
  - is either:

- (i) of historical or symbolic significance in relation to the proposed recipient; or
  - (ii) holds other special significance for the proposed recipient, and there are compelling reasons to justify its gifting to that recipient; or
  - (iii) of low value and
    - a. otherwise uneconomical to dispose of; or
    - b. the gifting supports the achievement of an Australian Government policy objective.
- (3) If a gift of property is being contemplated, the delegate is to consider whether authorising in a particular case would create an onerous or undesirable precedent. If the gift would create that precedent, it must be refused.

*Example:* If it would be difficult, in equity, for the Commonwealth not to authorise other requests for such gifts and which would in that way lead to significant losses of Commonwealth revenues.
- (4) For this reason, the delegate would need publicly defensible and objective grounds to justify favouring the person or organisation with the gift, ahead of other potential recipients.

### **3 Reasonable estimate to be obtained**

- (1) A delegate must not exercise the power under section 66 of the Act before obtaining a reasonable estimate of the market value of the relevant property proposed to be gifted.
- (2) If this is not possible, the delegate must use their discretion in assigning a notional value, and must record the basis for determining the value of the property.

## DELEGATIONS

### FINMAN 2 – Financial Delegations Manual

#### SCHEDULE 14 Delegation to approve the loan or hire of relevant property

1	Provision	PGPA Act section 15
2	Summary of function or power	To approve the loan or hire of relevant property

##### Delegates

Position	Limit of delegation
CDF	Unlimited
SES Band 3, O-9 (3 Star)	Unlimited
SES Band 2, O-8 (2 Star)	Unlimited
SES Band 1, O-7 (1 Star)	Unlimited
COMASC (O-6 or lower)	Unlimited
COMD DNSDC (VCDFG-JLC)	Unlimited
DSCS (VCDFG-JLC)	Unlimited
DEOS (VCDFG-JLC)	Unlimited
JLC Unit Commander / Commanding Officer (VCDFG-JLC)	Unlimited
COFS (O-6)	Unlimited
Regional Director Defence Support (EIG)	Unlimited
Base Support Manager (EIG)	Unlimited
Assets Stores & Inventory Manager (EIG)	Unlimited
Financial Adviser (overseas)	Unlimited
EL 2, O-6 (COL(E))	Unlimited
EL 1, O-5 (LTCOL(E))	Unlimited
COMDT (O-6)	Unlimited
ADF Unit Commanding Officer	Unlimited
ADF Unit Second in Command	Unlimited
ADF Unit Quartermaster/Maritime Logistics Officer/Logistics Officer	Unlimited
Logistics Manager / OIC Logistics Operations ADF	Unlimited
Contract Manager / Contract Services Manager (VCDFG-JLC)	Unlimited
Warehousing and Distribution Officer (APS 5)	Unlimited
Fleet Manager / Fleet Services Manager	Unlimited
OPSO MP COY, 1 MP BN	Unlimited

##### Secretary's Directions

1. The delegate must ensure that the loan or hire is in accordance with DI(G) LOG 4-3-012 – *Hire and Loan of Stores and Equipment to and from Sources Outside Defence*, as appropriate.
2. The delegate may approve the loan of Relevant Property to another Commonwealth agency free of charge or the hire of Relevant Property at full cost recovery, without reference to other authorities (see FINMAN 4 – *Resource Costing Manual: Usage Costs for Defence Resources and Assets* for full cost recovery rates).
3. Where the loan or hire is proposed at less than full cost recovery, a submission must be made to, and approval given by, an official holding a delegation under FINMAN 2 schedule 16 in accordance with the directions in that schedule.

**Note:** This delegation does not apply where the loan or hire of the relevant property is for the provision of Defence assistance to the civil community.

## DELEGATIONS

**Note:** This delegation does not apply where the loan or hire of Defence property is for the performance of contractual requirements in a contract between Defence and a contractor, and the contract specifies the conditions on the loan or hire. In such a case the PGPA Act section 23(3) delegate (Schedule 1) approves the loan or hire as part of the original contracting process.

## DELEGATIONS

### FINMAN 2 – Financial Delegations Manual

## SCHEDULE 15 Delegation to approve the disposal of relevant property

<b>1</b>	<b>Provision</b>	PGPA Act section 15
<b>2</b>	<b>Summary of function or power</b>	To approve the disposal of relevant property. This includes the disposal of relevant property with a value of nil

### Delegates

Position	Limit of delegation	Note
CDF	Unlimited	Note 1
SES Band 3, O-9 (3 Star)	Unlimited	Note 1
SES Band 2, O-8 (2 Star)	Unlimited	Note 1
SES Band 1, O-7 (1 Star)	Unlimited	Note 1
COMASC (O-6 or lower)	Unlimited	
EIG Official holding a LAA delegation	Unlimited	Note 4
OIC PSF Butterworth	Unlimited	Note 4
DLOG-A	Unlimited	
DGSC (VCDFG – JLC)	\$5,000,000	
DSCS (VCDFG – JLC)	\$3,000,000	
COMD DNSDC (VCDFG – JLC)	\$3,000,000	
COMD JLU (V) (VCDFG – JLC)	\$3,000,000	
JLC Unit Commanding Officer (VCDFG – JLC)	\$2,000,000	
Logistic Manager – DNSDC (EL 1, O-5) (VCDFG – JLC)	\$2,000,000	
DEOS (VCDFG – JLC)	\$500,000	Note 2
JLC Unit Second in Command	\$500,000	
Financial Adviser (Overseas)	\$500,000	
JLC Unit OIC (O-5)	\$500,000	
Director (EL2) Australian Military Sales Office (AMSO)	\$500,000	
EL 2, O-6 (COL(E))	\$500,000	
COMDT (O-6)	\$500,000	
COFS (O-6)	\$500,000	
JLC Contract Managers APS6	\$250,000	
Regional Director Defence Support (EIG)	\$200,000	
Assistant Director (EL1) Australian Military Sales Office (AMSO)	\$200,000	
ADF Unit Commanding Officer	\$200,000	
EL 1, O-5, (LTCOL(E))	\$200,000	
DDEOSD (VCDFG – JLC)	\$100,000	Note 2
JLC Fleet Managers (APS 6, O-4)	\$100,000	
Executive Officer Resource Asset Accounting (CFOG)	\$100,000	
Fleet Manager (CIOG)	\$100,000	
Fleet Manager (EIG)	\$100,000	
ADF Unit Second in Command	\$100,000	
ADF Unit Quartermaster/Maritime Logistics Officer/Logistics Officer	\$100,000	
OIC Logistics Operations ADF	\$100,000	
OC Domestic Policing Unit-Army	\$100,000	

**DELEGATIONS**FINMAN 2 – *Financial Delegations Manual*

Position	Limit of delegation	Note
JLC Regional Fleet Staff (APS 5, O-3)	\$75,000	
EO (APS 6) Australian Military Sales Office (AMSO)	\$50,000	
Contract Manager AAVNTC	\$50,000	
Warehousing and Distribution Officer (APS 5)	\$50,000	
JLC Disposal Manager (APS 4, O-2)	\$50,000	
OPSO MP COY, 1 MP BN	\$50,000	
O-3 Domestic Policing Unit-Army	\$50,000	
WO Coordination School of Military Engineering	\$50,000	
The officer in charge of a museum at EL2, O-6, EL1, O-5 level	\$10,000	Note 1
ADF Unit RQMS / SNCO Supply (SNCO SUP)	\$5,000	Note 3
APS6, O-4 (MAJ(E)) (CASG)	\$100,000	

**Notes:**

- Only these delegates may approve the disposal of Heritage and Cultural Assets.
- The delegation for munitions/explosive ordnance is 'Unlimited'.
- For Army, the delegate must be formally posted into the RQMS position and must have completed a Subject 4 WO2 (Unit Resources) Course / Subject 4 Warrant Officer, Operator Unit Supply Manager Course.
- Limited to the disposal of an interest in land (such as the surrender of a lease).

**Secretary's Directions**

- Disposal of relevant property may be by sale, trade-in, swap/exchange, transfer, dumping, destruction or abandoning. This includes the disposal of relevant property that is surplus, unserviceable or obsolete, including property which has a value of nil.
- The delegate must calculate the value of the property to be disposed of in accordance with FINMAN 1: Accounting Policy Manual.
- Where it is economical to do so, relevant property is to be disposed of by:
  - transferring the property (with or without payment) to another Commonwealth entity with a need for the property; or
  - selling the property at market price.
- If the property cannot be transferred or sold, any disposal must be an efficient, effective, economical and ethical use of public resources that is not inconsistent with the policies of the Australian Government.

**Note:** Only an official holding a delegation under the *Lands Acquisition Act 1989* may approve the disposal of land or an interest in land.

**Note:** This delegation does not apply where the relevant property is to be disposed of as a gift.



**DELEGATIONS****SCHEDULE 16 Delegation to determine charges for Defence supplied goods and services**

<b>1</b>	<b>Provision</b>	PGPA Act section 15
<b>2</b>	<b>Summary of function or power</b>	To determine rates and charges for goods, services or property provided or lent by Defence. To approve the waiving of charges for goods, services or relevant property provided or lent by Defence

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>	<b>Note</b>
CDF	Unlimited	
CFO	Unlimited	
FASRA	Unlimited	
ASFC	Unlimited	Note 1
DBSA (CFOG)	Unlimited	Note 1
HI (EIG)	Unlimited	Note 2
ASPM (EIG)	Unlimited	Note 2
HDSO (EIG)	\$50,000	Note 2
Regional Director Defence Support (EIG)	\$50,000	Note 2
CFO Associate Secretary Organisation (ASFM)	\$50,000	Note 3
Group CFO (CASG)	\$50,000	Note 3
Director Business Operations (Regions) (EIG)	\$50,000	Note 2
Head Defence Industry	\$50,000	Notes 1 and 4

**Notes:**

1. To determine rates and charges and to approve the waiving of charges up to \$50,000.
2. For cost waivers for the provision of facilities/estate assets only.
3. For cost waivers only.
4. Limited to matters relating to Defence Industry sponsored activities only.

**Note:** the delegate must ensure that a request for cost waiver up to \$50,000 has resource implication comments or advice provided by the Group Chief Finance Officer, or an official authorised by the Group Chief Finance Officer, prior to submission for approval.

**Note:** the delegate must ensure that a request for cost waiver in excess of \$50,000 has resource implication comments or advice provided by the CFO, or an official authorised by the CFO, prior to submission for approval.

**Secretary's Directions**

1. The delegate must ensure that a request for cost waiver up to \$50,000 has resource implication comments or advice provided by the Group Chief Finance Officer, or an official authorised by the Group Chief Finance Officer, prior to submission for approval.
2. The delegate must ensure that a request for cost waiver in excess of \$50,000 has resource implication comments or advice provided by CFO, or an official authorised by CFO, prior to submission for approval.
3. Where estate assets are involved, the delegate must comply with DI(G) ADMIN 35 - 1 - *Procedures for the use of Defence Estate assets by non-Defence organisations or individuals including commercial contractors.*

**Note:** This delegation does not apply to:

- (a) Defence Assistance to the Civil Community; or
- (b) the provision of government furnished equipment to contractors and other organisations providing services to Defence.

## DELEGATIONS

### SCHEDULE 17 Delegation to approve quotations for commercial work

<b>1</b>	<b>Provision</b>	PGPA Act section 15
<b>2</b>	<b>Summary of function or power</b>	To approve quotations for commercial work

#### Delegates

<b>Position</b>	<b>Limit of delegation</b>
CDS	Unlimited
DCDS	\$2,000,000
Chief of Division	\$200,000
Manager Scientific Engineering Services	\$200,000

#### Notes:

Any inquiries delegates may have about exercising this delegation should be directed to the DSTG Business and Commercialisation Office, which can also assist with the development and acceptance of commercial work.

#### Secretary's Directions

- The delegate may approve a quotation for less than full cost recovery in exceptional circumstances. Exceptional circumstances could include doing work for Australian industry in direct support of an ADF or wider-Defence project, providing assistance to a foreign Government or where there is a strong desire to undertake the work to gain some later leverage or advantage. Where less than full cost recovery is approved the reasons must be recorded by the delegate.

## DELEGATIONS

### FINMAN 2 – Financial Delegations Manual

#### SCHEDULE 18 Delegation to waive charges for Defence Assistance to the Civil Community

<b>1</b>	<b>Provision</b>	PGPA Act section 15
<b>2</b>	<b>Summary of function or power</b>	To approve the waiving of charges for goods and services provided by Defence through Defence Assistance to the Civil Community, including Defence assistance for Public Events of Significance

#### Delegates

<b>Position</b>	<b>Limit of delegation</b>	<b>Note</b>
CDF	\$100,000	Note 1
CA	\$100,000	Note 1
CAF	\$100,000	Note 1
CN	\$100,000	Note 1
CFO	\$100,000	Note 1
CJOPS	\$100,000	Note 1
DCJOPS	\$100,000	Note 1
VCDF	\$100,000	Note 1
Deputy Secretary CAS	\$100,000	Note 1
HMSC	\$100,000	Note 1
DCA	\$50,000	Note 2
DCAF	\$50,000	Note 2
DCN	\$50,000	Note 2
HNPAR	\$50,000	Note 2
HDSO (EIG)	\$50,000	Note 2
HI (EIG)	\$50,000	Note 2
Local Commander/Administrator or Senior ADF Officer	\$2,500	Note 3

#### Notes:

1. A request for cost waiver must have resource implication comments or advice provided by FASRA prior to submission for approval.
2. A request for cost waiver must have resource implication comments or advice provided by the Group Chief Finance Officer prior to submission for approval.
3. To waive the recovery of net additional costs associated with Defence Assistance to the Civil Community (DACC) category 5 only.

#### Secretary's Directions

1. The delegate must ensure that a request for cost waiver, where full cost exceeds \$100,000 is submitted to the Defence Minister.
2. The delegate must comply with the instructions detailed in the Defence Assistance to the Civil Community Manual.
3. The delegate must ensure that a request for cost waiver submitted to the Minister includes resource implication comments or advice provided by CFO, or an official authorised by CFO, prior to submission for approval.

## DELEGATIONS

### SCHEDULE 18A Delegation to be satisfied that the Consolidated Revenue Fund is appropriated for the repayment

<b>1</b>	<b>Provision</b>	Schedule 1 part 11 of the <i>Public Governance, Performance and Accountability (Finance Minister to Accountable Authorities of Non-Corporate Commonwealth Entities) Delegation 2014</i> (PGPA Act section 77)
<b>2</b>	<b>Summary of function or power</b>	To be satisfied that the Consolidated Revenue Fund is appropriated for the repayment

#### Delegates

Position	Limit of delegation
CFO	Unlimited
FASRA (CFOG)	Unlimited

#### Finance Minister's Directions

#### Scope of delegation

- (1) The delegate may only be satisfied that the Consolidated Revenue Fund is appropriated for the repayment under section 77 where:
  - (a) there is no other appropriation for the repayment; and
  - (b) the amount was remitted to the Official Public Account as an administered receipt; and
  - (c) the repayment cannot be greater than the amount originally received by the Commonwealth.
- (2) The delegate cannot be satisfied that the Consolidated Revenue Fund is appropriated for the purpose of section 77 when the repayment relates to:
  - (a) a departmental item; or
  - (b) a special account; or
  - (c) any other special appropriation which is available.

**DELEGATIONS****DIVISION 5 – Delegations under the *Legal Services Directions 2005*****SCHEDULE 19 Delegation to settle claims by or against the Commonwealth**

<b>1</b>	<b>Provision</b>	PGPA Act section 23(3)
<b>2</b>	<b>Summary of function or power</b>	To settle claims by or against the Commonwealth. This delegation applies to the handling of a monetary claim by or against the Department, other than a claim that needs to be determined under a legislative mechanism (such as a COMCARE benefit) or under a mechanism provided by contract (such as, an arbitration of a disputed contractual right), or a claim that is payable under Defence's Comcover insurance, or a normal claim for goods and services

**Delegates**

<b>Position</b>	<b>Limit of delegation</b>	<b>Note</b>
Associate Secretary	Limit of Funds Available	
Deputy Secretary CAS	Limit of Funds Available	
CFO	Limit of Funds Available	
Deputy Secretary Estate and Infrastructure	Limit of Funds Available	
Deputy Secretary People Strategies and Policy	Limit of Funds Available	
Head Defence Legal	Limit of Funds Available	
General Counsel CASG	Limit of Funds Available	
General Counsel Defence Legal	Limit of Funds Available	
Assistant Secretary Legal Services	Limit of Funds Available	
Director General ADF Legal Service	Limit of Funds Available	
HPP (DPG)	Limit of Funds Available	
HDSO (EIG)	Limit of Funds Available	
Head Reform and Corporate Services (EIG)	Limit of Funds Available	
FASDPS	Limit of Funds Available	
DGPS (DPG)	Limit of Funds Available	Note 1
DGPPEC	Limit of Funds Available	Note 1
DDWR	\$25,000	Note 1
Director Insurance	\$25,000	Note 2
Assistant Director Insurance	\$25,000	Note 2
DGFR (DPG)	\$25,000	Note 3
DCR (DPG)	\$25,000	Note 3
DLIT	\$25,000	
National Practice Manager Defence Legal	\$25,000	
COMASC	\$25,000	
Director People Policy Reform (DPPR)	\$25,000	
DPMPP	\$10,000	Note 1
Insurance Claims Manager	\$10,000	Note 2
Financial Adviser (overseas)	\$10,000	
SES Band 3, (O-9) 3 Star	No financial limit	
SES Band 2, (O-8) 2 Star	No financial limit	

**DELEGATIONS**FINMAN 2 – *Financial Delegations Manual*

SES Band 1, (O-7) 1 Star	No financial limit	
ADF Unit Commanding Officer or higher ADF rank	No financial limit	

**Notes:**

1. For claims relating to workplace relations issues.
2. For claims relating to minor insurance issues.
3. Limit of funds available for Human Rights and Equal Opportunity Commission claims.

**Secretary's Directions (excluding CASG Officials)**

1. Before exercising this delegation, the delegate must be reasonably satisfied that the proposed expenditure (if any) under the settlement:
  - promotes the proper use and management of public resources of Defence (i.e is efficient, effective, economical and ethical)
  - is not inconsistent with the policies of the Commonwealth, and
  - is covered by sufficient available appropriation.
2. The delegate must comply with any relevant instructions detailed in the Legal Services Directions issued by the Attorney-General pursuant to section 55ZF of the *Judiciary Act 1903*.
3. The delegate must handle claims in accordance with legal principle and practice.
4. The delegate should seek legal advice as appropriate, and must ensure that Defence's interests are protected and settlements are appropriate.
5. A claim over \$25,000, including a claim with any related claims totalling over \$25,000, is a major claim and must be referred through Defence Legal to the Australian Government Solicitor or a legal provider on the Defence Legal Panel for advice that settlement of it would be in accordance with legal principle and practice.
6. The delegate must seek financial clearance (including funds availability) from the Chief Finance Officer of the group which will incur the expenditure prior to approving settlement of a claim.
7. The delegate must not settle a claim in relation to CASG.

**Secretary's Directions for CASG Officials**

8. An official exercising this delegation is a 'Section 23 Commitment Approval Delegate' for the purposes of PGPA Act Section 23 (3). A separate approval is not required under FINMAN Delegation Schedule 1 - To approve the commitment of relevant money.
9. Before exercising this delegation, the delegate must be reasonably satisfied that the proposed expenditure (if any) under the settlement:
  - promotes the proper use and management of public resources of Defence (i.e is efficient, effective, economical and ethical)
  - is not inconsistent with the policies of the Commonwealth, and
  - is covered by sufficient available appropriation.
10. A delegate must also (where relevant e.g. where a claim is funded centrally) obtain financial clearance (including confirming funds availability) from Director Strategic Fiscal Advice before exercising this delegation.
11. In all cases, before approving a settlement, the delegate must be satisfied that the proposed settlement terms appropriately protect Defence's (and the Commonwealth's more widely) financial, legal and other interests in the circumstances. It is a requirement to seek legal advice before the exercise of a delegation, in certain circumstances, as discussed below.

12. A delegate must not exercise this delegation unless satisfied that the settlement complies with the Legal Services Directions 2005 (Directions).
13. A principal requirement of the Directions is that claims (other than a claim that needs to be determined under a legislative mechanism (such as a COMCARE benefit) or under a mechanism provided by contract (such as an arbitration of a disputed contractual right), or a claim payable under Defence's insurance cover with COMCOVER), must only be settled in accordance with legal principle and practice.
  1. For this purpose, a delegate must carefully assess and weigh in the balance a range of relevant matters; the purpose in each case being to determine that the proposed settlement achieves an outcome that advances the Commonwealth's legal, financial and other interests. Relevant matters that a delegate should take into account include:
    2. the merits of the Commonwealth's position
    3. the range of possible and likely outcomes if the matter was pursued in court
    4. further costs likely to be incurred by Defence if the claim is not settled
    5. the terms of the proposed settlement
    6. any prejudice or other consequences for Defence or the Commonwealth more widely of settling the claim on the proposed terms, and
    7. the desirability or advantages of clarifying the law.
  8. A settlement must not be effected merely because of the cost of defending what is clearly a spurious claim.
  9. Consistent with the requirements of the Legal Services Directions 2005, including the exemption to Appendix C of the Directions granted to DMO on 2 February 2010:
  10. In cases with a settlement value of \$25,000 or less, a delegate may exercise this delegation on the basis of a common sense view that the proposed settlement is in accordance with legal principle and practice.
  11. In cases where the settlement is between \$25,000 and \$2.5 million a delegate may settle a claim without seeking external legal advice. If external legal advice is not obtained, a delegate must obtain written legal advice from a CASG Legal Deputy Counsel that the proposed settlement is in accordance with legal principle and practice and seek approval from the General Counsel CASG.
  12. In cases where the settlement value is greater than \$2.5 million, a delegate must obtain written legal advice from an external legal service provider that the proposed settlement is in accordance with legal principle and practice.
  13. Within 30 days of the end of each financial year, officials holding this delegation must give to CASG Legal a written certificate confirming that the powers and functions exercised under this delegation comply with the Directions. This confirmation must include:
    14. details of any apparent or possible breach of the Directions not previously reported and of which the delegate is aware
    15. details of any actions taken during the financial year to address the causes of any reported breaches of the Directions, and
    16. any other information considered relevant to Defence's compliance with the Directions.

## DELEGATIONS

### SCHEDULE 20 Delegation to approve financial assistance to an official for legal proceedings

1	Provision	PGPA Act section 23(3)
2	Summary of function or power	To approve the payment of financial assistance for legal proceedings in which a Defence official is involved where, at the time of the alleged event or occurrence giving rise to the legal proceedings, the individual was a Defence official

#### Delegates

Position	Limit of delegation	Note
Associate Secretary	Limit of Funds Available	Note 1
Chief Finance Officer	Limit of Funds Available	Note 1
Deputy Secretary CAS	Limit of Funds Available	
Head Defence Legal	Limit of Funds Available	
General Counsel CASG	Limit of Funds Available	
Defence General Counsel	Limit of Funds Available	
Assistant Secretary Legal Services	Limit of Funds Available	
Director General ADF Legal Service	Limit of Funds Available	
Director, Litigation	Limit of Funds Available	
Deputy Director, Litigation	Limit of Funds Available	

#### Notes:

1. The delegate must seek independent legal advice before exercising this delegation.

#### Secretary's Directions

1. The delegate must comply with the Legal Services Directions issued by the Attorney-General pursuant to section 55ZF of the *Judiciary Act 1903*.
2. The delegate must not approve a proposal for the commitment of relevant money to unless satisfied, after reasonable inquiries, that giving effect to the proposal:
  - (i) would be an efficient, effective, economical and ethical use of public resources that is not inconsistent with the policies of the Australian Government; and
  - (ii) is covered by sufficient available funds or appropriation.



## DELEGATIONS

### SCHEDULE 21 Delegation to approve payments for the provision of emergency legal services to ADF members overseas

<b>1</b>	<b>Provision</b>	PGPA Act section 23(3)
<b>2</b>	<b>Summary of function or power</b>	To approve the payment of emergency legal services to ADF members overseas where delay in obtaining legal services will jeopardise the member's legal rights

#### Delegates

<b>Position</b>	<b>Limit of delegation</b>
Associate Secretary	\$15,000
Head Defence Legal	\$15,000
Director General ADF Legal Service	\$15,000
Commander Australian Contingent*	\$15,000
Head Australian Defence Staff, Defence Attaché or Defence Advisor	\$15,000
J06/Director Legal Headquarters Joint Operations Command	\$15,000

#### Notes:

- \* Commander Australian Contingent includes a commander joint task force, a commander task force, a commander Australian contingent or other contingent commander, an ADF commanding officer, detachment commander or national commander, not below the rank of O-4.

#### Secretary's Directions

- The delegate must advise the recipient that the provision of emergency legal services does not guarantee that the recipient will be entitled to or granted legal assistance at Commonwealth expense.
- The delegate must not approve a spending proposal unless satisfied, after reasonable inquiries, that giving effect to the spending proposal:
  - would be an efficient, effective, economical and ethical use of public resources that is not inconsistent with the policies of the Australian Government; and
  - is covered by sufficient available funds or appropriation.

## DELEGATIONS

### FINMAN 2 – Financial Delegations Manual

## DIVISION 5A – Other Delegations

### SCHEDULE 21A Delegation to prescribe certain persons as officials of the Department of Defence

<b>1</b>	<b>Provision</b>	PGPA Act section 13(3)(c) PGPA Rule section 9
<b>2</b>	<b>Summary of function or power</b>	To prescribe certain persons as officials of the Department of Defence

#### Delegates

<b>Position</b>	<b>Limit of delegation</b>
CDF	Unlimited
Associate Secretary	Unlimited
SES Band 3, O-9 (3 Star)	Unlimited
SES Band 2, O-8 (2 Star)	Unlimited
SES Band 1, O-7 (1 Star)	Unlimited

#### Secretary's Directions

- The delegate may issue an instrument in writing to a consultant or independent contractor, where all of the following apply:
  - The individual is as an independent consultant or contractor or is an employee of an independent consultant or contractor engaged to provide services to Defence;
  - The contracted services require the exercising of a delegation under FINMAN 2;
  - The individual or employee is capable of being identified by name in relation to the exercising of the delegated power(s).
- Financial Limits and Conditions applicable to the delegated power(s) must be established by delegate subject to the limits set by the Secretary in the relevant FINMAN 2 delegation schedule. When setting the monetary limit in the instrument in writing, the delegate should ensure that it is appropriate to the level, functions and responsibilities of the prescribed official.
- The delegate may consult with another official prior to issuing an 'Authority to Act' in relation to determining the requirement to prescribe an individual as an official for the purposes of exercising delegated powers as well as obtaining details of any relevant competencies required for the exercising of delegated powers.
- The delegate must understand and comply with all requirements specified in:
  - [RMG No. 212](#) 'Prescribing officials for non-corporate Commonwealth entities',
  - [The relevant delegations schedules in](#) FINMAN 2, and
  - [DPPM Chapter 1.4.](#)
- The instrument in writing is to use the template in FINMAN 5.

# AUTHORISATIONS

## PART B - AUTHORISATIONS

### DIVISION 6 – Authorisation under the *Judiciary Act 1903*

#### SCHEDULE 22 Authorisation to bring a suit on behalf of the Commonwealth

<b>1</b>	<b>Provision</b>	<i>Judiciary Act 1903</i> Section 61
<b>2</b>	<b>Summary of function or power</b>	Authorisation to bring a suit on the behalf of the Commonwealth

#### Authorised officials

Position	Limit of authorisation
Associate Secretary	Unlimited
CFO	Unlimited
Head Defence Legal	Unlimited
General Counsel Defence Legal	Unlimited
General Counsel CASG	Unlimited
Assistant Secretary Legal Services	Unlimited
Director General ADF Legal Service	Unlimited
Deputy Secretary Estate and Infrastructure	Unlimited
DLIT	Unlimited
DGPS (DPG)	Unlimited
HDSO (EIG)	Unlimited
NECPO (EIG)	Unlimited
ASPM (EIG)	Unlimited
CJLOG (VCDFG-JLC)	Unlimited
Inspector General	Unlimited
Assistant Secretary General Investigations and Review (IG)	Unlimited
Director Investigations and Recovery (IG)	Unlimited

#### Secretary's Directions

1. The authorised official must comply with the Legal Services Directions issued by the Attorney-General pursuant to section 55ZF of the *Judiciary Act 1903*.
2. The authorised official must sign, date and print their name and position, and indicate "For and on behalf of the Secretary of Defence".

**Note:** If the Department wishes to institute proceedings in the name of the Commonwealth the proceedings may only be instituted by an official authorised under this Schedule.

## AUTHORISATIONS

### DIVISION 7 – Authorisation under the Constitution

#### SCHEDULE 23 Authorisation to approve Compensation for Detriment Caused by Defective Administration

<b>1</b>	<b>Provision</b>	Constitution section 61 & 64
<b>2</b>	<b>Summary of function or power</b>	To approve on the behalf of the Minister for Defence, the payment of Compensation for Detriment caused by Defective Administration (CDDA Scheme)

##### Authorised officials

<b>Position</b>	<b>Limit of authorisation</b>
Secretary	Limit of Funds Available
Deputy Secretary, Estate and Infrastructure	Limit of Funds Available
Head Defence Legal	Limit of Funds Available
General Counsel Defence Legal	Limit of Funds Available
Defence Special Counsel Defence Legal	Limit of Funds Available
Director General ADF Legal Service	Limit of Funds Available
Director Special Financial Claims	\$25,000

##### Defence Minister's Directions

1. The officials listed are authorised, for and on behalf of the Minister for Defence, to approve payments under the Compensation for Detriment caused by Defective Administration (CDDA) scheme.
2. The officials are authorised, for and on behalf of the Minister for Defence, to accept, partially accept or reject a claim for compensation under the scheme.
3. An official addressing or processing a claim or an authorised official considering a decision relating to a claim under the Scheme must comply with the relevant provisions of the applicable legislation, government policy, Accountable Authority Instructions and other Defence instructions, and the directions set out in the Schedules.
4. An official exercising an authorisation under this schedule is also exercising a power as an approver for the purposes of PGPA Act section 23(3).
5. Approval is only to be given as "For and on the behalf of the Minister for Defence".

## AUTHORISATIONS

FINMAN 2 – *Financial Delegations Manual*

### Division 8 – Authorisation under the *Public Governance, Performance and Accountability Act 2013*

#### SCHEDULE 24 PGPA Act section 23(1) authorisation for Special Purpose Aircraft

1	<b>Provision</b>	<i>Financial Management and Accountability (Finance Secretary to Chief Executive of Department of Defence) Delegations 2014-15, (PGPA Act section 110)</i>
2	<b>Summary of function or power</b>	Execute a Contract for the purpose of the Charter Agreement – Special Purpose Aircraft dated 28 July 2004

#### Authorised officials

Position	Limit of authorisation
CDF	Unlimited
CFO – Air Force	Unlimited
Comd 1JMOVGP	Unlimited
BM-ALG	Unlimited
Official with procurement duties issuing a purchase order	Unlimited

#### Secretary's Directions

1. The authorised official must sign "for and on behalf of the Secretary of Defence".

## GLOSSARY

The following definitions apply to terms used in this manual.

### **Accountable assets**

Accountable assets are assets with an acquisition value less than the capitalisation threshold and over which Defence chooses to implement tracking or resource planning controls.

### **Accountable and reportable assets**

Accountable and reportable assets are assets whose acquisition cost exceeds the relevant asset capitalisation threshold.

### **Accountable authority**

The accountable authority for Defence is the Secretary of Defence (PGPA Act section 12).

### **Agency agreement**

Agency agreement, for the purpose of procurement, means an agreement for the procurement of goods and/or services under which an agency is obliged, or may become obliged, to make a payment of relevant money to another agency.

### **Amount owing**

An amount owing to the Commonwealth includes an amount that is owing, but is not yet due for payment.

### **Arrangement**

An arrangement includes a contract, agreement, deed or understanding.

### **Asset**

An asset is a resource:

1. controlled by an entity as a result of past event; and
2. from which future economic benefits are expected to flow to the entity.

### **Asset register**

Asset register includes any record of relevant property, including inventories of consumable items held in stock, for which the department is accountable.

### **Business Manager**

For the purpose of financial delegations, a Business Manager is a position delivering business management services, who is required to exercise financial delegations and make decisions on financial resources to achieve outcomes for a business area. Business Manager includes a Director, Business Management, Director, Resources Management, or similar position.

### **COMASC**

COMASC is the Commander of an Australian Contingent overseas. COMASC includes the Commander of a Joint Task Force and the Commander of an Australian contingent of a UN led or other mission. COMASC does not include an official posted to and working in an Australian Embassy or High Commission.

### **Commonwealth Credit Card**

Commonwealth credit card means a credit card issued to the Commonwealth to enable the Commonwealth to obtain cash, goods or services on credit. Commonwealth Credit Card includes the Defence Purchasing Card, the Defence Travel Card, a fuel card and Cabcharge Card.

### **Debt**

A debt is a sum of money which is:

1. ascertained or capable of ascertainment;
2. now payable or will become payable in the future by reason of a present obligation; and
3. can be recovered in an action for debt.

### **Debtor**

A debtor is a person who has a debt to the Commonwealth. Debtors' accounts can also be referred to as *accounts receivable*.

### **Defence civilian**

As defined in Section 3 of the *Defence Force Discipline Act 1982* (DFDA), Defence civilian means a person (other than a Defence member) who:

1. with the authority of an authorised officer as defined in the DFDA, accompanies a part of the ADF that is:
  - (a) outside Australia; or
  - (b) on operations against the enemy; and
2. has consented, in writing, to subject themselves to ADF discipline while so accompanying that part of the ADF.

### **Defence employee**

Defence employee means a person employed in the Department of Defence under section 22 of the *Public Service Act 1999* (the Public Service Act).

### **Defence member**

Defence member, as defined in section 3 of the DFDA, means:

1. a member of the Permanent Navy, the Regular Army or the Permanent Air Force; or
2. a member of the Reserves who:
  - (a) is rendering continuous full-time service; or
  - (b) is on duty or in uniform.

### **Direction**

A direction is an instruction issued by the Secretary relating to the exercising of a delegated power with which a delegate must comply.

### **Equivalent**

For the purposes of delegated authority under Part 6 of Delegation Schedule 1 means:

1. An official of equal level or rank, and,
2. Where the duties and responsibilities of the position are similar, and,
3. There is an ongoing and regular requirement to exercise a delegation for the higher delegated financial limit.

### **Ex-officio**

Delegations are issued *ex officio* – that is, they are issued to an office or position, or class of positions, rather than to a person. Delegations may be exercised by the holder of the position, or an official occupying or performing the duties of the position.

### **Financial Adviser**

A Financial Adviser may be appointed for an operation, exercise, project or remote post, where infrastructure does not exist to support financial and administrative requirements for Defence personnel.

### **Financial Task**

Financial task:

1. means a task or procedure relating to the commitment, spending, management or control of relevant money; and
2. does not include a task or procedure of that kind that is performed by an outsider, under an agreement or arrangement authorised under section 29 of the PGPA Rule.

### **Financial Framework (Supplementary Powers) Act**

The *Financial Framework (Supplementary Powers) Act 1997*, as amended from time to time.

### **Full cost**

Full cost, for the purpose of cost recovery or cost waivers, is the total cost of all resources used in producing an output, that is, the total of direct and indirect costs. Costs such as those involved in

policy development, meeting parliamentary service functions, financial reporting, etc cannot be included when determining an amount for cost recovery or cost waivers.

### **Funds available**

Funds available are: funds allocated through the departmental budget management process,  
minus: expenditure, liabilities and commitments to date against the funds allocated,  
minus: other obligations expected to be incurred in the ordinary course of business (such as, staffing and other ongoing costs, etc).

### **Group Head**

A Group head is any senior manager or Service chief who reports directly to the Secretary or the Chief of the Defence Force, and any other official identified by the Secretary as a Group Head.

### **Heritage assets**

Heritage assets are assets identified by the Government for preservation because of their unique historical, geographical, cultural or environmental attributes.

### **ICT Hardware**

ICT Hardware includes:

- desktop hardware (e.g. desktop computers, monitors, laptops, tablets, notebooks);
- mobile ICT (e.g. BlackBerry, DREAMS tokens);
- voice and video support (e.g. fixed telephones, mobile telephones, smartphones, satellite telephones, telecards, pagers, wireless data cards, Secure Mobile Environment – Personal Electronic Devices, private automated branch exchanges, DSN Unified Communications, Voice Over Internet Protocol, teleconferencing equipment, audiovisual equipment including smartboards, projectors and smart televisions, videoconferencing equipment including Top Secret, Top Secret/Secret, Secret, Secret/Unclassified and Unclassified);
- all associated equipment such as SIM cards;
- peripherals capable of connecting to Defence ICT systems, (e.g. multifunction devices, network printers, plotters, scanners, facsimile machines, upload devices including card readers);
- computer accessories (e.g. assistive technology, CD/DVD burners, switch boxes for multiple computers, portable storage devices such as thumb drives);
- storage (including storage arrays – Networked Attached Storage Devices and Storage Area Networks);
- backup (e.g. backup equipment and tapes);
- servers (e.g. mainframes, X86, and Unix such as AIX, Solaris and Linux);
- network infrastructure (e.g. racks, fixed cabling, UPS, environmental equipment);
- communications equipment (e.g. switches, routers, media converters, load balancers); and
- appliances (e.g. vendor provided black box solutions).

### **Indemnity**

An indemnity is a legally binding promise whereby a party undertakes to accept the risk of loss or damage another party may suffer - an indemnity arrangement includes a deed of indemnity, and any indemnity arrangement or clause in a contract, agreement or arrangement whereby the Commonwealth agrees to indemnify the contractor or other party, or a third party.

### **Inventories**

Inventories are items held in store for distribution.

### **Limit of Funds Available**

LOFA is: limit of funds available (see also Funds available).

### **Official**



An official is a person who is in an agency, and includes an employee under the Public Service Act and an Australian Defence Force member. Delegations to officials in the delegation schedules are to Defence officials unless otherwise stated.

**Official account**

An official account is an account with a bank for the receipt, custody, payment or transmission of relevant money, either inside or outside Australia.

**Other CRF money**

Other CRF money is money that forms part of the Consolidated Revenue Fund (CRF) other than relevant money or any other money of a kind prescribed by the PGPA Rule.

**PGPA Act**

The *Public Governance, Performance and Accountability Act 2013*, as amended from time to time.

**PGPA Rule**

The *Public Governance, Performance and Accountability Rule 2014*, made by the Finance Minister under section 101 of the PGPA Act, as amended from time to time.

**Relevant money**

Relevant money is:

1. money standing to the credit of any bank account of the Commonwealth or a corporate Commonwealth entity; or
2. money that is held by the Commonwealth or a corporate Commonwealth entity.

(PGPA Act section 8).

**Relevant property**

Relevant property is:

1. property (other than relevant money) that is owned or held by the Commonwealth or a corporate Commonwealth entity; or
2. any other thing prescribed by the PGPA Rule.

(PGPA Act s 8).

**Spending proposal**

Spending proposal means a proposal that could lead to the creation of a contract, agreement or arrangement under which relevant money is payable or may become payable (including relevant money that is payable or may become payable in circumstances in which payment would be a notional payment for the purposes of section 76 of the PGPA Act).

**Standing offer**

Standing offers are arrangements under which a number of potential suppliers, usually selected through a single procurement process, may each supply property or services to an Entity as specified in the standing offer.

**Travel Card**

The Defence Travel Card is a credit card issued to the department to enable the department to obtain on credit goods and/or services related to travel.

**Unit**

Unit includes a formation headquarters, a school/college and a ship, and for the purpose of AAIs and financial delegations, an independent unit commanded by an officer of O-3 level or higher not reporting directly to an O-4 or O-5 level officer.

**Unit Commander**

Unit Commander/Commanding Officer includes a Defence Attaché. For the purpose of the asset management AAIs, a Unit Commander includes a military or civilian Defence member appointed as a Commander/Manager of an asset holding entity, and a contract authority.

## **FINMAN 5**

### **5 COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS**

#### **5.1 INTRODUCTION**

##### **5.1.1 About this FINMAN 5 Chapter**

**5.1.1.1** The processes and procedures described below provide guidance for officials to achieve the policy outcomes defined in AAI 5 - *Commonwealth Credit Cards and Credit Vouchers* and should be read with the supporting guidance referred to in section 5.1.2.

##### **5.1.2 References**

**5.1.2.1** The following policy and guidance is additional to that provided in AAI 5 – *Commonwealth Credit Cards and Credit Vouchers* and this FINMAN 5 chapter:

- a) DI(G) CIS 6–7–002 Mobile Telephones and Related Services
- b) DI(G) FIN 12-1 – The Control of Fraud in Defence and the Recovery of Public Monies
- c) DI(G) PERS 25-7 – Gifts, Hospitality and Sponsorship
- d) Defence Procurement Policy Manual (DPPM)
- e) Electronic Supply Chain Manual (ESCM)
- f) Department of Finance Resource Management Guide (RMG) No. 416 'Facilitating Supplier Payment through Payment Card'
- g) AAI 1 'Managing Risk and Internal Accountability'
- h) FINMAN 5 chapter 1 'Managing Risk and Internal Accountability'
- i) AAI 7 'Managing Relevant Money'

#### **5.2 DEFENCE CREDIT CARDS AND CREDIT VOUCHERS**

**5.2.1.1** Defence Credit Card means a Commonwealth credit card or credit voucher, which is issued to enable an official to obtain cash, goods or services on credit for the purpose of official Defence business, and includes:

- a) Defence Purchasing Card (DPC);
- b) Defence Travel Card (DTC);
- c) Fuelcard;
- d) Cabcharge Card/E-Ticket;
- e) Telecard; or
- f) other similar credit cards issued by Defence for the purpose of official Defence business.

##### **5.2.2 Entering into Credit Card Agreements**

**5.2.2.1** A credit card agreement with a credit card service provider may only be entered into by the Chief Finance Officer or another delegate mentioned in FINMAN 2 schedule 6.

**5.2.2.2** The agreement must require the money to be repaid within 90 days after Defence is notified by the lender of the amount borrowed.

##### **5.2.3 Coincidental Private Expenditure**

**5.2.3.1** In limited circumstances it is acceptable for a Defence Official to use a Defence Credit Card for Coincidental Private Expenditure. If a Defence Credit Card has been used for Coincidental Private Expenditure, the card holder must repay the amount of the Coincidental Private Expenditure within 30 days and prior to verification of the expenditure within the Card Management System (CMS).

**5.2.3.2** Coincidental Private Expenditure on a Defence Credit Card means expenditure for a private purpose that is:

- a) necessary,

FINMAN 5 Chapter 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

- b) unavoidable,
- c) directly linked with; and
- d) coincidental to;

expenditure for the purpose of official Defence business. Coincidental Private Expenditure must reflect a single claim comprising official business elements and personal elements that cannot be separated and be authorised by an appropriate financial delegate.

**5.2.3.3** When paying an account that has both official and Coincidental Private Expenditure a card holder should separate the accounts and use the Defence Credit Card for official charges only. Members must take reasonable steps to ensure personal expenses can be separately settled, prior to incurring the expense.

**5.2.3.4** If a Defence Credit Card has been used inadvertently for private expenditure, the amount is repayable as a debt owed to the Commonwealth immediately the inadvertent use becomes known and prior to verifying the expenditure in the Card Management System (CMS).

**5.2.3.5** A Defence credit card holder must not gain any personal benefit from the use of the card. For example, the card must not be used in conjunction with personal purchasing reward plans such as FLYBUYS.

**5.2.3.6** If the card holder separates from Defence, or moves to a position which does not require a card, the card holder must advise the issuing authority and surrender (or destroy) the card. If the card is a DPC or DTC, then the surrender (or destruction) must be undertaken in accordance with the Defence Corporate Cards Frequently Asked Questions.

**5.2.4 Fraudulent Use of Defence Credit Cards**

**5.2.4.1** Fraudulent or suspected fraudulent use of a credit card must be reported without delay to Defence Investigative Authority in accordance with DI(G) ADMIN 45–2 *The Reporting and Management of Notifiable Incidents*. Additional guidance can be obtained from DI(G) FIN 12-1 – *The Control of Fraud in Defence and the Recovery of Public Monies*.

**5.2.4.2** **Defence Investigative Authority** means the Australian Defence Force Investigative Service (ADFIS), the three service police organisations of the Army, Navy and Air Force that report to the Provosts Marshal, the Directorate of Security Intelligence and Investigations (SII) within the Defence Security Agency (DSA) and the Directorate of Investigation and Recovery (DIR) within the Inspector General Division.

**5.2.5 Key governance elements of Credit Card management**

**5.2.5.1** Credit Cards are an important and commercially sensible method of transferring funds to Defence's Vendors. It is Government policy that all payments to vendors less than \$10,000 should be by Credit Card unless a vendor does not accept a Credit Card (See RMG No. 416).

**5.2.5.2** Defence Travel Card (DTC) spending limits are set at \$10,000 on a default basis. Business cases for increased limits are to be provided to Group CFO's (or their representative) for approval. Credit Card limits may be reduced below the default limit depending on usage patterns.

**5.2.5.3** Defence Purchase Card (DPC) spending limits are set at \$30,000 on a default basis. Business cases for increased limits are to be provided to Group CFO's (or their representative) for approval. Purchase Card limits may be reduced below the default limit depending on usage patterns.

**5.2.5.4** Virtual Card spending limits are set at \$500,000 on a default basis. Business cases for increased limits are to be provided to Group CFO's (or their representative) for approval. Virtual Card limits may be reduced below the default limit depending on usage patterns. Virtual Travel Cards are to be used only when transaction volumes demand or as determined by the Group CFO.

FINMAN 5 Chapter 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

- 5.2.5.5** The Group CFO's (or their representative) will annually (first quarter of each financial year) review the following to determine whether to retain or alter:
- a) Individual Credit Card spending limits
  - b) Individual Credit Card cash withdrawal limits
  - c) Virtual Credit Card limits
  - d) Merchant Categories
  - e) Unused Credit Cards
- 5.2.5.6** Business areas can request a change of credit limit if required by sending Web Form *AE602 Corporate Card Application and Limit Amendment* to their GCFO for approval before sending the completed and approved form to Defence Credit Cards.
- 5.2.6 Cash Withdrawals Using a Defence Credit Card**
- 5.2.6.1** Cash withdrawals using a DPC are only to be used as a last resort, where:
- a) the vendor cannot be entered on ROMAN; or
  - b) a Defence Credit Card cannot be utilised.
- 5.2.6.2** Cash withdrawn using a Defence credit card is an advance of relevant money. AAI 7 - *Managing Relevant Money* and its associated FINMAN 5 chapter define policies and procedures for approving and managing an advance including the requirement for the Advance Holder to hold appropriate drawing rights to operate the advance.
- Note: Cash withdrawn by an official using a DTC for approved defined entitlements, such as meals and incidentals, is not an advance of relevant money and therefore not subject to AAI 7 - Managing Relevant Money. Using the DTC to pay direct to the supplier for these entitlements is encouraged.*
- 5.2.6.3** An official who has withdrawn cash (which is relevant money) is personally responsible for the advance until it is acquitted. Loss or partial loss of an advance constitutes a loss of relevant money (see AAI 7 - *Managing Relevant Money* and its associated FINMAN 5 chapter).
- 5.2.6.4** Should a DPC holder require access to cash withdrawal and therefore require a PIN, a business case must be sent to the GCFO using the AE602 form, outlining the requirement to have cash access. GCFO approval may only be sought after the approval of the AAI 7 delegate for the establishment of the cash advance has been obtained.
- 5.2.6.5** Purchasing card cash withdrawal limits are set at \$0 on a default basis. Business cases for increased limits are to be provided to Group CFO's for approval.
- 5.2.6.6** Transactions will appear in the CMS and require coding in the normal manner.
- 5.2.6.7** DPC fees and interest charges for cash withdrawals are charged at the Group level. DTC fees for cash withdrawals are charged at the cost centre level.
- 5.2.7 Defence Purchasing Card (DPC) and Defence Travel Card (DTC)**
- 5.2.7.1** Financial Services Division in the Chief Finance Officer Group is the contract manager for the DPC and the DTC. Deputy Secretary Estate and Infrastructure Group is the technical authority for the Defence travel program.
- 5.2.7.2** Groups are responsible for including the operation of DPC and DTC into risk management strategies and fraud control plans.
- 5.2.7.3** Responsibilities of card holders include the following:
- a) comply with the relevant bank's card usage conditions for the DPC;
  - b) comply with Diners Club card usage conditions for the DTC;
  - c) comply with Defence's guidelines outlining the appropriate standards for the spending of relevant money;
  - d) retain invoices/receipts for DPC transactions. Diners Club DTC transactions are tax compliant and therefore hard copies of invoices are not required, while MasterCard DTC transactions are not tax compliant and therefore require

FINMAN 5 Chapter 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

- receipts. However officials are encouraged to retain hard copies of invoices for record keeping and ease of travel acquittal. Receipts are also not required for purchases made using cash withdrawn from the DTC for meals and incidentals, except where cash is used for accommodation to allow for GST redemption;
- e) maintain their card and card details in a safe place, including ensuring that if recorded, the PIN is not located in such a way as to be associated or available on or near the card; and
  - f) report a lost/stolen card immediately to the issuing financial institution and the card holders supervisor.
- 5.2.7.4** Where a credit card is used to make a purchase on the internet, card holders should take reasonable steps to ensure they are purchasing from a reputable site, and that it utilises standard internet security, such as the encryption of payment data. This is often represented by a padlock shown in the web browser. Where a card holder is unsure of the validity or security of the site, they should seek alternate means of procuring the goods.
- 5.2.8 Expenditure Approvals for Defence Purchasing Card (DPC) and Defence Travel Card (DTC)**
- 5.2.8.1** When using the DPC, expenditure approval is to be recorded by the FINMAN 2 schedule 1 delegate on the invoice/receipt provided by the merchant or a form such as the AC977 *Credit Card Purchase Authorisation* for the purpose of complying with the recording requirements of section 18 of the *Public Governance, Performance and Accountability Rule 2014*. This approval must be obtained prior to committing the Commonwealth, including booking travel, or any other travel related costs, e.g.. flights, accommodation, passports, visas, third party notes, etc.
- 5.2.8.2** When using the DTC, expenditure approval is recorded on an overseas budget calculator as part of the overseas visit authority (OVA), the domestic travel budget calculator and authority, the SLG domestic budget calculator and authority, iTravel or the AE505 Travel Request Form as per the appropriate type of travel to be undertaken.
- 5.2.9 Payment Verification for Defence Purchasing Card (DPC) and Defence Travel Card (DTC)**
- 5.2.9.1** Transactions must be processed in the CMS within 60 days of the transaction appearing in the CMS to comply with Group due diligence reporting requirements. Some travel suppliers expense transaction instantly, in these instances a traveller may verify the transaction prior to travel.
- 5.2.9.2** If a transaction is disputed, the DTC card holder has 60 days and the DPC card holder has 90 days after the transaction has been loaded into the CMS to dispute the transaction. Transactions outside of these time periods cannot be disputed.
- 5.2.9.3** It is a Group responsibility to ensure that structures in the CMS are accurate and the cardholders are attributed to the correct administration centre.
- 5.2.9.4** Groups are ultimately responsible for clearing all outstanding CMS transactions. In the absence of supporting documentation (eg receipts and invoices) for a CMS transaction, Groups are to take all reasonable steps to verify the transaction with the applicable area/unit.
- 5.2.9.5** Where the investigation of a CMS transaction without supporting documentation confirms the claim's validity, the card holder is required to provide a statutory declaration in relation to the expenditure. It is the responsibility of the Group to clear the transaction and document their verification steps.
- 5.2.10 Role of CMS Supervisors**
- 5.2.10.1** CMS Supervisors:

FINMAN 5 Chapter 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

- a) have visibility of CMS profiles of the cardholders they are responsible for,
- b) are responsible for ensuring the cardholders they are responsible for process CMS transactions within 60 days of the transactions appearing on CMS (emails will be sent to CMS Supervisors notifying them of their cardholders' outstanding CMS transactions); and
- c) are not required to check and approve cardholder transactions on CMS.

**5.2.11 Using the Defence Purchasing Card (DPC)**

**5.2.11.1** The DPC should be used where it can be demonstrated that doing so provides value for money and the proposed purchase is not subject to other requirements.

**5.2.11.2** The DPC is to be used for low value, low risk purchases. It may also be used for urgent requirements or unforeseen circumstances in an operational situation (refer sub para 5.2.9.3g). Where the procurement needs to contain specific terms and conditions, a Purchase Order is to be raised. The DPC terms and conditions are standard and cannot be varied as required by the card holder.

**5.2.11.3** The DPC should not be used by card holders in the following situations:

- a) procurement that requires the agreement of terms and conditions that differ from those that are commercially available;
- b) procurement where the preferred supplier does not accept payment by DPC;
- c) procurement where standard terms under a Purchase Order represent better value for money (eg where a premium is imposed by the supplier for use of the credit card);
- d) payment of items procured through the Military Integrated Logistics Information System (MILIS);
- e) payment of items procured through ROMAN; and
- f) the purchase of items of supply that are deployable or support an operational capability. These should be purchased through MILIS except under exceptional circumstances such as extreme urgency. Where the DPC is used to purchase an item of supply that is deployable or supports an operational capability, the DPC Checklist contained in ESCM, volume 5, section 7, chapter 4 is to be completed, and action must be taken to have the item brought to account in MILIS by Electronic System Purchase Order as soon as practicable (refer ESCM, volume 5, section 7, chapter 4, annex A, DPC and DMOPC Process Flow).

**5.2.11.4** It is not permitted under any circumstances to split purchases to circumvent expenditure limits on a Defence Credit Card.

**5.2.11.5** For all purchases where the DPC is not used, a Purchase Order is to be raised.

**5.2.11.6** Contractors, consultants or professional service providers may hold DPCs provided their duties require them to do so and they are prescribed officials under the PGPA framework.

**5.2.12 Using the Defence Travel Card (DTC)**

**5.2.12.1** The DTC is issued to staff that have a reasonable expectation of undertaking business travel as part of their official duties.

**5.2.12.2** The DTC is used to pay for all expenses as approved in the travel budget, including, but not limited to:

- a) accommodation;
- b) hire cars, taxis, ferries, trains, buses and other surface transport;

FINMAN 5 Chapter 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

- c) meals;
- d) incidentals; and
- e) air travel.

- 5.2.12.3** After-travel certification is only required where there is a change to the approved travel plan that changes the original travel budget. Changes to the travel plan may result in the requirement to either document the additional travel that was approved by a delegate or the repayment of money withdrawn inadvertently prior to the travel plan changing.
- 5.2.12.4** Defence credit card transactions must be acquitted by the account holder through CMS within 60 days of a transaction appearing on CMS in accordance with Accountable Authority Instruction (AAI) 5.3.1.13.
- 5.2.12.5** Once Defence credit card transactions are acquitted on CMS, they will automatically be approved in the system.
- 5.2.12.6** Contractors, consultants or professional service providers cannot hold a DTC.
- 5.2.13 Fuelcards**
- 5.2.13.1** The Joint Fuels and Lubricants Agency (JFLA) manages the Defence Fuelcard system and is responsible for issuing policies and directions associated with the use of the Fuelcard. All users of Defence vehicles, transport supervisors, commanders and authorising officers have a responsibility to ensure the Defence Fuelcard is used and controlled in accordance with promulgated instructions.
- 5.2.13.2** Fuelcards can only be used to purchase fuel where it is not practical to obtain these products from Defence sites.
- 5.2.13.3** Defence Fuelcards are deemed to be a credit card and bound by the regulations applicable to Commonwealth-provided credit cards. This applies whether the Fuelcard is issued by a commercial fuel supplier, a commercial card provider or the Defence Fuelcard administrator.
- 5.2.13.4** The Commanding Officer or Officer Commanding of a Defence Unit, or their civilian equivalents, has an obligation to monitor Fuelcard usage and to ensure that transactions against each Fuelcard are reconciled on a monthly basis. ESCM volume 5, section 7, chapter 1 identifies procedures for the proper use of Fuelcards.
- 5.2.13.5** A card holder should report a lost or stolen Fuelcard to the office which issued the card.
- 5.2.13.6** Primary responsibility for proper Fuelcard use lies directly with the official who is issued with the card (i.e. the card holder).
- 5.2.14 Telecards**
- 5.2.14.1** Defence-issued telephone credit cards (Telecards) are usually only issued to individuals, or units for reissue to on-call staff, on either a temporary or permanent basis, as required, to meet operational or business needs. As they attract costs in addition to call costs, users are not to use Defence-issued Telecards to make calls on Defence or private mobile telephones.
- 5.2.14.2** Staff should discuss their communications options with their respective Data Voice Manager (DVM). A check of the mobile telephone coverage at the destination may indicate that a Telecard is more appropriate than a mobile telephone with international access and global roaming and, in any event, should be issued to an overseas traveller, whether carrying a mobile or not. It is particularly important for personnel travelling internationally on business to be aware that a number of countries do not have reciprocal access agreements with Australian carriers for global roaming.
- 5.2.14.3** Officials who are issued with a Telecard and PIN are not to pass the card or divulge the card number or PIN to any person without local DVM written approval in each individual circumstance.
- 5.2.15 Document Retention**

FINMAN 5 Chapter 5 – COMMONWEALTH CREDIT CARDS AND CREDIT VOUCHERS

- 5.2.15.1** It is a Group responsibility to ensure that all signed Defence Credit Card documentation is retained on an official departmental file. *See AAI 1 - Managing Risk and Internal Accountability* and its associated FINMAN 5 chapter.
- 5.2.16 Forensic Monitoring and Controls**
- 5.2.16.1** In line with the PGPA Act 2013 cardholders should be aware that the controls, assurance activities and compliance checks conducted by Directorate of Financial Assurance and Compliance (DFAC), CFO Group will continue.
- 5.2.16.2** This means that cardholders may be required to provide their travel documentation to DFAC for review at any time.