[redacted]

BRIEF FOR a/FASICTSDR: ICTPA Periodic Refresh RFT Release	
Group: **CIOG**	Reference:
Through: ED ICTCBS	Due Date: 24 February 2023

References

A. ICTPA Periodic Refresh Procurement Plan (February 2023)

Recommendation

That you:

a) **Approve** the release of the ICTPA Periodic Refresh Request for Tender (RFT) in accordance with Reference A.

Background

1. In accordance with Reference A, the ICTPA Periodic Refresh RFT release documentation including the Conditions of Deed and attachments, Conditions of Tender and attachments, and all reference material relevant to this Periodic Refresh RFT have been finalised.

2. As the Delegate of the ICTPA Periodic Refresh activity, FASICTSDR approval is required to grant release of the RFT (page 19 of Attachment A) via AusTender.

3. The following advisers have endorsed the ICTPA Periodic Refresh RFT:

a. Australian Government Solicitors (AGS) appointed ICTPA Periodic Refresh probity advisors,

b. Norton Rose Fulbright (NRF) appointed ICTPA Periodic Refresh legal advisors,

c. NMP – CIOG appointed ICTPA Periodic Refresh procurement advisors.

Consultation

Kate Brophy – Senior Executive Lawyer, AGS

s22 [redacted] s47E(d) [redacted] Executive Director ICT Commercial and Business Services 22 February 2022	a) APPROVED / PLS DISCUSS s22 [redacted] s47E(d) [redacted] a/FASICTSDR 22 February 2022
Responsible Officer s47E(d) [redacted]	W: Mob: s22 [redacted]

Attachments:

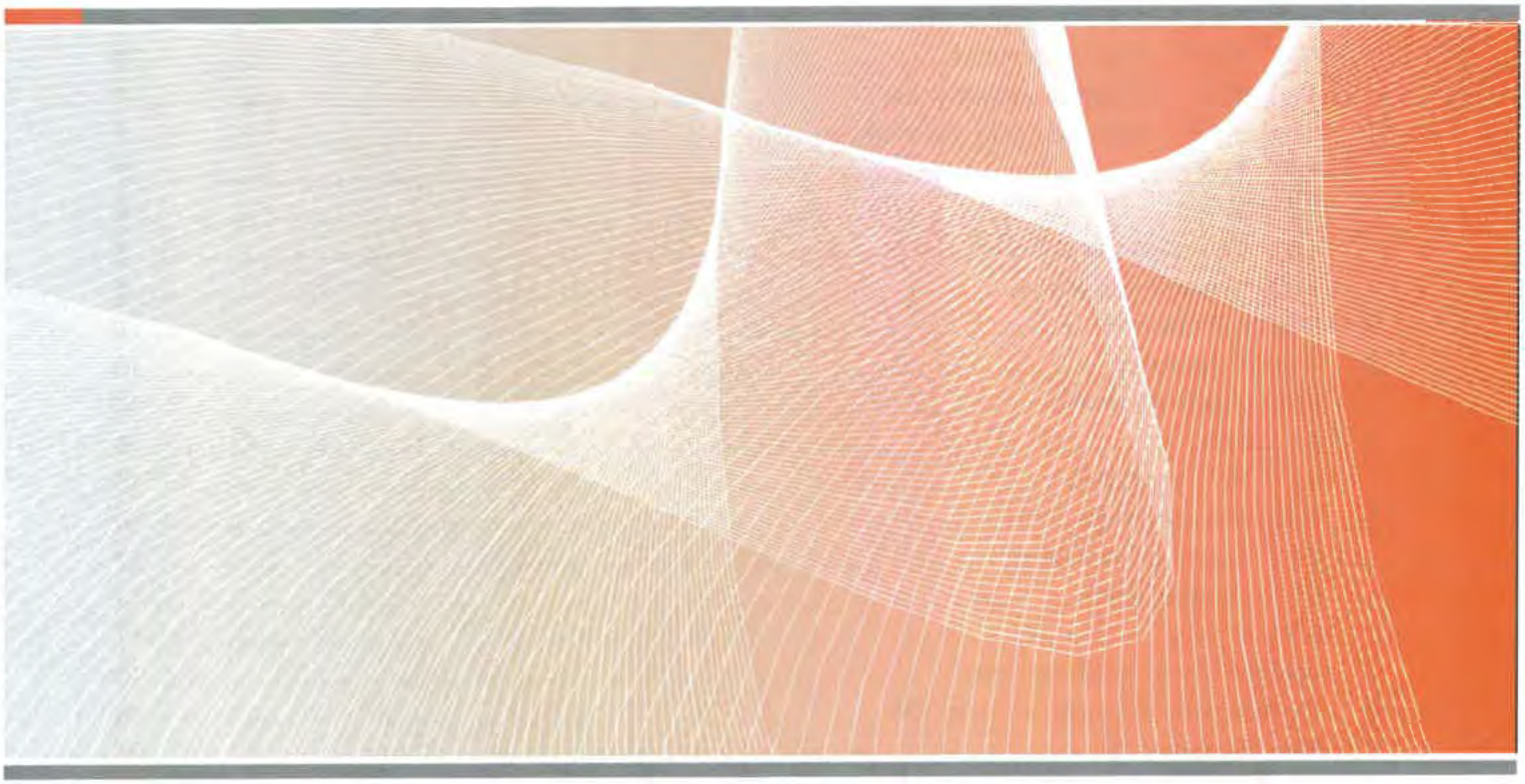
A.

[redacted]

Australian Government
Department of Defence
Chief Information Officer Group

ICTPA Periodic Refresh

Procurement Plan



s47E(d)

Director – Panel and Supplier Governance, ICTCBS
ICT Service Delivery and Reform Division

Contents

Table of Figures

Table of Tables

1. Introduction

The purpose of this document is to describe the procurement approach for information and communication technology Suppliers to participate in the Information Communications and Technology Provider Arrangement (ICTPA) Periodic Refresh. This Periodic Refresh looks to open market opportunities multiple times a year which will allow new suppliers to tender for access to the panel and allow current suppliers the opportunity to tender for additional skills or modules not currently held.

The Plan also addresses the method of procurement with a justification for the approach selected, the governance of the procurement process, procurement risk management methodology and procurement schedule.

Approval of the Plan will enable the project team to progress the activities outlined to achieve the objectives of this procurement activity.

1.1 Background

The Department of Defence (Defence) introduced ICTPA on 13th July 2018 as the primary panel arrangement to source goods and services in support of its information and communications technology (ICT) environment following the expiry of the Applications Managed Services Partnership Agreement (AMSPA).

The 2016 Provider Arrangement Sourcing Strategy (Sourcing Strategy) recommended options to extend ICTPA in accordance with the Deed at end of years 5, 8 as well as multiple Refreshes over the term of the panel:

- if one of four predefined conditions exist (i.e. services being unavailable, demand for service not being met, value for money not being realised, or specific skills not available)

The 2021 ICTPA Refresh was undertaken in line with the four predefined conditions of the 2018 Panel Deed. The Refreshed Deed, executed at 30 September 2021, amended the Panel Refresh process set out in the Panel Deed to allow the Commonwealth to make changes to the structure, terms, operations and other aspects of the Panel from time to time. The ICTPA Periodic Refresh may involve undertaking a Panel Refresh from time to time in line with conditions set in the ICTPA Conditions of Deed clause 2.9 (Panel Refresh).

Defence has decided to extend the initial Deed Term for a period of three years in accordance with the options provided for in the Panel Deeds executed as a result of the original RFT. Accordingly, the expiry date for the existing Deed Term will be 24 June 2026. During the term of the extension it is proposed to conduct Periodic Refreshes of the panel in accordance with this Procurement Plan.

The proposed Periodic Panel Refresh is considered necessary to maintain currency of supplier's offerings and capture new supply markets established post previous approaches to market to meet the Commonwealth's ongoing and evolving business and military requirements.

This provides benefit by adding additional suppliers to the ICTPA through an approach to market, and allowing incumbent suppliers to expand their opportunities for service offerings.

1.2 Vision

The Defence vision is that ICTPA will enable it to become a smarter and more sophisticated buyer of ICT goods and services through the 'implementation of a new structural framework supported by approach-to-market, commercial, transition and sustainment strategies'. This document builds upon this vision, through the broadening (scope and participation) and maturation (operation) to add the dimensionalities of affordability, quality, flexibility and relevance.

1.2.1 Broadening

Expand ICTPA to reflect:

- industry capability,
- emerging technologies, and
- in-demand service offerings.

1.2.2 Maturation

Develop ICTPA in-line with the Sourcing Strategy, focusing on:

- service and Supplier categorisation,
- benefits monitoring and realisation,
- support for Defence First Principles Review and ITIL 4.

1.3 Structure of the Plan

1.3.1 This Plan describes the process and governance arrangements that Defence will follow in undertaking all future Periodic Refresh procurements in accordance with the Conditions of Deed clause 2.9 (Panel Refresh). In particular, it describes;

a) the project background, personnel resourcing requirements, and estimated budget including costing assumptions;

b) procurement activities, deliverable and its timelines and relevant assumptions and dependencies;

c) the methodologies that will be used to determine VFM and assess and mitigate risks associated with each procurement process and any resultant contract; and

d) associated governance arrangements pertaining to each procurement activity.

1.4 Outcomes

This document maintains references from the 2021 ICTPA Refresh Program in the ICTPA Business Case[1] and Defence ICT Strategic Direction 2016:2020[2] and more recent 2022 Defence ICT Strategy to identify the outcomes sought from continual Periodic refresh activities.

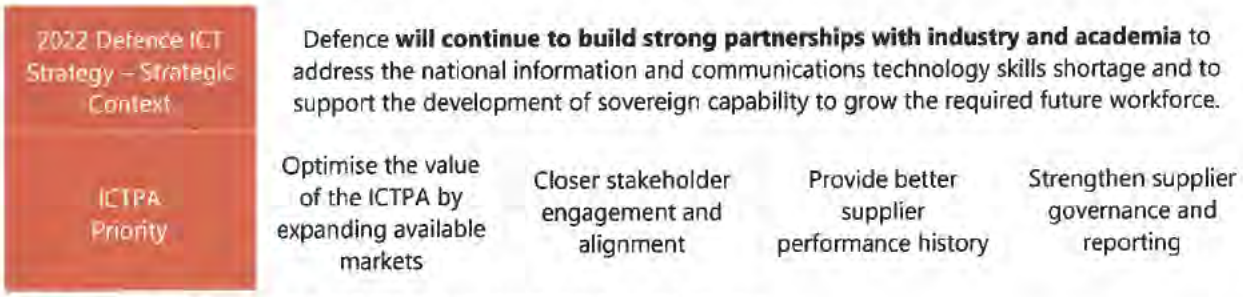


Figure 1. ICTPA Periodic Refresh Activity Outcomes aligned to 2022 Defence ICT Strategy

The ICTPA Periodic Refresh aims to maintain and extend the ecosystem that allows ICT procurement within the Department of Defence (Defence) to deliver affordable, high quality and flexible services to business that

[1] ICTPA Business Case, March 2016
[2] Defence ICT Strategic Direction 2016:2020, August 2016

also provides Value for Money (VfM) to the Commonwealth. The Periodic Refresh will continue to iteratively mature ICTPA in line with its foundation Adaptive Sourcing Framework and Sourcing Strategy, focusing on;

a. service categorisation

b. supplier categorisation

c. benefits monitoring and realisation

d. Continuing currency with the SFIA adopting future states as required

1.5 Strategic Alignment

1.5.1 Sourcing strategy principles

ICTPA's sourcing strategy principles have been revisited and considered during the development of the Refresh Strategy. Below captures those revisited principles and acknowledges those achieved and looks to consider Periodic Refresh adjustments in support of the original Refresh,

2016 Sourcing Strategy Principle	Refresh Alignment
Flexible Commercial Constructs	Refine service and Supplier categorisation *(minor achievement)* **Periodic Refresh** – Continue to redefine supplier offer to service categorisation as opposed to supplier tiering.
Maintain Competitive Landscape	Increased industry SME participation and broader subcategory representation *(achieved)* **Periodic Refresh** – Draws on the Refresh success and opens more regular opportunity for supplier growth.
Strategic Partner Alignment	Increase pre-procurement events *(not achieved)* **Periodic Refresh** – The multiple approaches per year, supported by the Deed Governance Framework will open more opportunities for industry engagement.
Innovation	Introduction of Supplier innovation score derived from supplied innovation measures *(not achieved)* **Periodic Refresh** – Continue development of innovation will be mapped as part of future strategy.
Incentivised Arrangements	Encourage appropriate use of incentivised arrangements as appropriate *(achieved)* **Periodic Refresh** - The Deed adopts multiple commercial options for users in achieving more complex contracting through incentive-based agreements.
Operating Model Alignment	Maintain and drive operating model maturity *(ongoing)*

Table 1. 2016 Sourcing Strategy Principles / Refresh Alignment

1.5.2 Supplier alignment

Significant opportunities exist to improve the mix and depth of Suppliers available to Defence and other agencies. This includes engaging new entrants with additional and niche skills resulting in an extended and comprehensive list of pre-qualified suppliers. The Periodic Refresh will also enable the participation of Suppliers who did not bid for ICTPA during the 2021/2022 Refresh, did not fully appreciate the quality of response required to furnish an acceptable offer or reasonably demonstrate capability for admission, or were unsuccessful in their latest attempt to gain admission to the ICTPA (or parts there-of).

1.5.3 Service Modules

By design the Service Modules remain broadly in the same construct as in the Refreshed 2021 ICTPA procurement process, and for the most part operate as originally designed. The Periodic Refresh may consider adjustments within the ICT Personnel Resources (ICTPR) Module. Further changes may be reflected in further documentation as outlined by the delegate. ICTPR is a direct translation of SFIA7 that allows users of the panel to access skilled workforces to deliver respective outcomes. The key gap here is a translation of ICT Service Categorisation (i.e. Cloud services) that can be easily identifiable by a suppliers Service Offering. It is becoming more unlikely that suppliers will have cross-skilled bench resources that can be pooled to meet the, sometimes erratic and without notice, demands of the Commonwealth. In place of skill selection placement it is much more effective to group suppliers in to agreed Service Categories for users of the Panel to access. This will be more attainable for suppliers as they can focus on Business Development and Offer to specific ICT market sections and not bear the weight of having to obtain skill specific resources as requested by Panel users.

1.5.4 Supplier performance

In accordance with ICTPA Deed section 6.1 (a)(i-v) the Supplier must provide the Services in accordance with the Deed and each work order, included by;

a) providing the Services and Deliverables by the relevant dates (if applicable) and in the manner required

b) achieving Acceptance or Approval (as applicable) of the Services and any Deliverables by the relevant dates (if applicable) and in the manner required.

c) achieving Milestones by the relevant milestone dates

d) achieving, or exceeding, the Required Performance Level for each Performance measure for each Review Period.

e) in relation to those Services to which no Performance Measure relates, achieving a level of performance that is no less than the best international industry standards and practices in ICT services that a supplier would achieve when providing services of the same type as those services.

1.5.5 Skills category alignment

Defence and many other participating agencies are contemplating the impact of the current Skills Framework for the Information Age (SFIA) 7 standard to ensure ICTPA remains current in providing access to new and emerging technologies and skills. Defence and many other agencies continue to consider the impact of technological advancement such as SFIA 8 and beyond where applicable.

1.6 Audience

The audience for this document includes the following key stakeholders:

- CIOG FAS ICT SDRD (The Delegate),
- CIOG Non-Material Procurement (NMP - CIOG)
- ICTPA Periodic Refresh Steering Committee, and
- Members of the Procurement Team

1.7 Scope

ICTPA is Defence's primary vehicle for the procurement of Application Services, ICT Services and Systems Integration Services. Periodic Refresh encompasses all services within service modules.

Service Modules	Definition
Application Services	Used to specify requirements related to the design, testing, operating and improvement of ICT assets and capabilities that are currently in operation. Within application services, the term 'application sustainment' is also used to refer to those activities that are ongoing, as opposed to those which are typically one-time activities to deliver an application and is referred to as 'application development' or 'DevOps'.
ICT Personnel Resources	Used to specify labour resource requirements. ICT Services sees the Supplier responsible for the provision of labour resources, to augment Defence's delivery model with specific skill sets, for a defined period.
Systems Integration	Used to specify requirements related to the management, definition, implementation, and integration of ICT assets (with an emphasis on the relationships between assets and Suppliers) to deliver a capability. Within systems integration, provision is made for the procurement of software, hardware and ancillary services to deliver the required end-to-end capability.

Table 2. ICTPA Service Modules Definition

1.8 Estimated Panel Value

The current estimated value of the ICTPA Panel is approximately $3.7 billion at $700 million per annum.

1.9 Out-of-Scope Items

Periodic Refresh out-of-scope items include all information and communications technology goods and services provided by mandated Whole of Government (WoAG) Panels.

2. About this Document

This Periodic Refresh Procurement Plan is compliant with the Commonwealth Procurement Rules (CPRs) and provides a fair approach to procuring services whilst providing value-for-money (VfM).

Outcome	ICTPA Approach	Result
Treat all Suppliers equally	Allow all Suppliers to be assessed from a common baseline.	Non-discriminatory policy towards all potential Suppliers to ensure that SMEs can engage in fair competition.
Engender trust and transparency	Provide visibility to Suppliers on the acquisition strategy and subsequent procurement processes.	Procurement plans and the assessment process must be publicly available.
Simplified processes	Minimise complexity of responding. Simplify BAU procurement activity.	CPRs require procurements to be efficient in the use of time, resources and achievement of outcomes.
Drive commercial outcomes	Create a competitive baseline of approved Suppliers to meet the future ICT needs of Defence.	CPRs encourage competition and is committed to sourcing at least 10% from SMEs.
Deliver value-for-money	Generate a panel of Suppliers with the ability to deliver Value for Money for Defence.	Achieving value for money is the core rule of the CPRs based on financial and non-financial costs and benefits.
Flexible and agile	Recognise and cater to the presence of constant change and evolution of the ICT services environment and consequently ICT Suppliers.	Procurements need to be effective in terms of achieving intended outcomes or results.

Figure 2. Periodic Refresh Procurement Plan and the CPRs

3. Refresh Approach

Periodic Refresh adopts industry expert practice, the CPRs and Defence's Procurement Policies and Guidelines to conduct a series of single stage procurements.

Stage One	Stage two	Stage three	Stage four	Stage five	Stage six
Planning	Request Documentation: RFT	Approach to Market: RFT	Evaluation: RFT	Negotiation	Contract Signature
ICTPA Periodic Refresh Methodology					
	Open Approach to Market			Evaluation and execution	
Develop Communications Approach	Develop Request Documentation: RFT	Release to Market. RFT	Evaluate Responses: RFT	Negotiate Deeds	Manage Supplier Deed Returns
	Implement Tooling: RFT	Develop Supplier Briefings: RFT	Develop Correspondence: RFT	Develop Correspondence	
		Manage Responses: RFT		Develop Contract Management Documentation	
		Develop Supplier: Communications RFT			

Figure 3. Periodic Refresh Approach

Periodic Refresh Stage	Description
Stage One **Planning** ICTA Periodic Refresh Methodology Open Approach to Market Develop Communications Approach	**Stage One. Planning** This stage will allow for the development of a Procurement Plan (ie this document) which sets out how the procurement will be undertaken, including defining the process that can be followed by the Commonwealth. A Risk Assessment may be developed to provide a plan or assessment which will include but will not be limited to, the identification of risks, the process, procedures and tools used to identify and capture risks, describe the impact of each risk, the specific risk criteria that would be affected by the risks and mitigating controls to manage those risks. Development of a Probity Framework (Reference B), a Probity Plan and conduct of Probity Briefing will define the strategy and approach by which Defence personnel will ensure effective probity risk management within the Project. The Probity Briefing will outline key probity principles and regulatory framework to key personnel involved with the procurement, including their respective obligations throughout the entire process. The objective of this phase is the development of a consultative Periodic Refresh procurement approach and schedule which is fit-for-purpose within Defence's operational context.
Stage Two **Request Documentation: RFT** ICTA Periodic Refresh Methodology Open Approach to Market Develop Request Documentation: RFT	**Stage Two. Request Documentation: RFT** Completion of Request Documentation: RFT documentation in accordance with the Complex Procurement Guide, Development of RFT Rate Cards and Tooling (OpenWindows SaaS) implementation. The objective of this phase is the completion of RFT documentation in preparation for industry engagement and release via the appropriate tender submission tool.
Stage Three **Approach to Market** ICTA Periodic Refresh Methodology Open Approach to Market Release to Market. RFT	**Stage Three. Approach to Market: RFT** Activation of the process by which industry will be engaged to complete a Request for Tender either as a New Supplier or Extant Supplier (indicating their intent to seek a change to their current scope of services). Extant Suppliers applying changes to their current scope are included in this activity as they will be required to undergo evaluation as to their suitability as a Supplier of service in their tendered areas. The objective of this phase is the completion of the RFT activity via the appropriate tender submission tool in-line with Complex Procurement guidelines and CPRs.

Periodic Refresh Stage	Description
Develop Supplier Briefings: RFT	
Manage Responses: RFT	
Develop Supplier: Communications RFT	
Stage Four Evaluation: RFT ICTA Periodic Refresh Methodology	**Stage Four. Evaluation: RFT** Assessment of RFT responses to qualify each Supplier's eligibility to provide service in their tendered areas. The objective of this phase is the evaluation of conforming RFT responses received to determine those eligible for admission to the ICTPA under the Periodic Refresh Conditions of Tender.
Evaluation and execution	
Evaluate Responses: RFT	
Develop Correspondence	
Stage Five Negotiation ICTA Periodic Refresh Methodology	**Stage Five. Negotiation** Referencing the approach to evaluating a Tenderer's eligibility to participate in the Periodic Refresh terms for negotiation are developed for each successful Tenderer. This includes the terms for negotiation. The objective of this phase is to clearly define the negotiation points for each Tenderer – including individual Negotiation and development of Contract Management documentation.
Evaluation and execution	
Negotiate Deeds	
Develop Correspondence	
Develop Contract Management Documentation	
Stage Six	**Stage Six. Contract Signature**

Periodic Refresh Stage	Description
Contract Signature	Management of the contractual basis upon which Defence will be qualifying Suppliers for admission to the panel. This includes return of the revised Deed, Contractual Schedules and Rate Cards. The objective of this phase is to manage the return of compliant signed contractual artefacts.
ICTA Periodic Refresh Methodology	
Evaluation and execution	
Manage Supplier Deed Returns	

Figure 4. Refresh Stage Description

4. Procurement Approach

Key Question	Response	Rationale
Is the procurement based on an identified need?	yes	ICTPA Periodic Refresh is supported by s47E(d) Executive Director, Chief Information Officer Group. The scope of the Refresh; • expanding the number, mix and quality of Suppliers
Is the method of the procurement known e.g. open or limited?	open	As a non-corporate Commonwealth entity, Defence is bound to comply with the CPRs. A Refresh RFT provides the greatest opportunity to identify Suppliers to deliver flexibility, innovation, competitive pricing and VfM. Due to the complexity and value of the Periodic Refresh, the procurement does not satisfy the conditions for processing as a limited or pre-qualified tender.
Is the complexity of the procurement known e.g. simple, complex?	complex	Periodic Refresh is a complex procurement that involves many people, several phases, requirements, documents, and a substantial amount of time, cost, effort, and risk. • Each Refresh will take in excess of 4-6 months to complete. • Each Refresh will cost about $136,000 dollars to complete. The price tag on the goods and/or services procured via the refreshed panel will be in excess of $200m per annum.
Is the procurement single-stage or multi-stage?	series of single stage	Periodic Refresh is to be released to industry as a series of RFTs. Qualification via RFT ensures Suppliers execute a standard Deed, and a common set of commercial and service-specific schedules aligned to the Deed.
What is the vehicle chosen to approach the market?	Tender Submission Tool	The RFT will be released on an appropriate tender submission tool with preceding notification announcements.

Table 3. Department of Finance Procurement Process Consideration

5. Evaluation

An evaluation will be undertaken to determine whether a Supplier should be appointed to the Panel for some or all of the services for which they have applied

The VfM factors considered are:

- Commercial, evaluating a Supplier's ability to comply with the commercial terms, and condition, policies and procedures (the Deed). The deed is intended to be non-negotiable so that it is common across suppliers on the panel.
- Technical (capacity and capability), innovation and experience, evaluating a Supplier's ability to strategically align with Defence in relation to the technical, and service requirements as well as past proven experience to ensure any Refreshed service provides value for money.
- Price, evaluating a Supplier's rates.
- Risk

Value for money will be achieved by an open approach to the market to identify the approach and methodology that best fit the strategic objectives of Defence and other Commonwealth agencies' requirement whilst also taking into account the technical, commercial and financial considerations that will:

a) use public resources in an efficient, effective, economical, and ethical manner that is not inconsistent with the policies of the Commonwealth (s15 & 21 of the Public Governance, Performance and Accountability Act 2013 (PGPA Act);

b) facilitate accountable and transparent decision making;

c) encourage appropriate engagement with risk;

d) be commensurate with the scale and scope of the business requirement; and

e) the evaluation criteria will consider the economic benefit of the procurement to the Australian economy as per paragraph 4.7 of the CPRs

5.1 RFT Evaluation

RFT Evaluation Teams are responsible for evaluating Supplier responses and final short-listing of RFT Suppliers for negotiation.

Organisation and Function	Workforce	Responsibilities
Chair and Deputy Chair	Internal	• Sign-off transparency and viability of the tender response evaluation.
Commercial	Internal	• Tenderer response 'commercial' evaluation.
Technical	Internal	• Tenderer 'technical' evaluation.

Figure 6. Refresh Stakeholder Input RACI

Organisation and Function	Workforce	Responsibilities
Financial	Internal	• Tenderer response financial viability and price evaluation.
Probity	External	• Advising Defence on the management of probity risk throughout the evaluation and negotiation process
Legal	External	• Tenderer response 'legal' evaluation
Initial Screening	NMP - CIOG	• Extraction of responses from AusTender • Loading of responses to evaluation tool • Conduct of initial screening

Table 4. Tender Evaluation Team Composition

The contract execution team are responsible for negotiating and the provision of specialist knowledge regarding Suppliers and services during contract execution. The contract execution team is comprised of key individuals of the tender evaluation team to ensure effective efficient processing of contract execution and artefacts.

6. Governance Arrangements

Formal governance arrangements underpin the Refresh to ensure compliance with prevailing CPRs, Commonwealth law and policies.

Figure 5. Procurement Governance Structure

Figure 6. Refresh Stakeholder Input RACI

6.1 Steering Committee

Provides strategic direction and leadership ensuring that the development and execution of the procurement plan is undertaken in a manner that meets the needs of Defence.

Governance Entity. Steering Committee	Responsibilities
• Membership. To be advised • Frequency of Meetings. Monthly	• Review and endorse key deliverables and recommendations made by the working group. • Provide and articulate overall project objectives and ensuring that it is aligned with the mission and imperatives. • Provide leadership for the Refresh leadership on behalf of the steering committee and sponsor. • Review progress against the Refresh work plan with a focus on delivery and the critical path. • Make timely decisions to Refresh risks and issues, making recommendations for items to be escalated to the steering committee. • Approve recommended change requests within project budget, contingency or make recommendations to the steering committee. • Ensure that the appropriate subject matter experts are actively engaged by the working group and involved in the relevant working session and workshops.

Table 5. Steering Committee Terms of Reference

6.2 Working Group

Provides tactical guidance and leadership to ensure that the Refresh is undertaken in a manner that meets the needs of Defence in becoming a more sophisticated and smarter buyer of ICT services.

Governance Entity. Working Group	Responsibilities
• Membership. To be advised • Frequency of Meetings. Monthly	• Tactical guidance and leadership to the project teams. • Review and validate documentation prior to presentation to the steering committee. • Maintain focus on the factors outside of the working group's control that is critical to its success. • Maintain the focus of the procurement activity on the Refresh scope outcomes and benefits.

Table 6. Working Group Terms of Reference

6.3 Probity

Provides advice on relevant aspects of Refresh, including reviewing the RFT documentation.

Figure 6. Refresh Stakeholder Input RACI

Governance Entity, Probity	Responsibilities
• Membership. To be advised • Frequency of Meetings. Weekly	• Prepare a probity plan, covering communications with key stakeholders, roles and responsibilities, administrative arrangements, conflict of interest etc. • Review all documentation, as the need arises, as well as other processes and practices. • Provide a final probity report and sign-off on the conduct of the process referencing the Probity Plan and the relevant procurement documentation. • Participate in meetings as requested by Defence. • Provide any other advice and sign-offs as may be reasonably requested by Defence. • Tactical guidance and leadership to the project teams in management of probity issues and risks.

Table 7. Probity Terms of Reference

7. Legislation and Standing Orders

Commonwealth Sourcing is governed by several acquisition policies, regulations and legislation. The Periodic Refresh process will comply with the appropriate and relevant Commonwealth laws and policies. The following documents including the relevant acquisition policies, regulations and legislations that have been considered in the development of this document.

8. Procurement Approvals and Sign-Off

Defence requires a robust and well-defined procurement approval process. Procurement Approval Gates represent events where the Delegate authorises progression to the next stage in the procurement process. Following approval of this Procurement Plan, each procurement undertaken under the Refresh process will require separate approvals for key steps as set out in the table of Procurement Approval Gates below:

Procurement Approval	Description
Procurement strategy	Approval granted, by <FAS ICT SDRD>, to undertake a Periodic Refresh activity as per the process defined in this Periodic Refresh Procurement Plan.

Figure 6. Refresh Stakeholder Input RACI

Procurement Approval	Description
Procurement Plan	Approval granted, by <FAS ICT SDRD>, for the development of documentation necessary to refresh the panel arrangement as per the process defined in this Refresh Procurement Plan.
Request for Tender	Approval granted, by <FAS ICT SDRD>, for the release to market of documentation necessary to refresh the panel arrangement as per the process defined in this Refresh Procurement Plan.
Tender Evaluation Plan	Approval granted by <FAS ICT SDRD>, after the release to market of documentation necessary to refresh the panel arrangement as per the process defined in this Refresh Procurement Plan.
Initial Screening Report	Approval granted, by <FAS ICT SDRD>, to begin the evaluation of the Suppliers that have responded in a correct format.
Evaluation Report	Approval granted, by <FAS ICT SDRD>, to select Suppliers that have met the qualifying threshold during the evaluation process for due diligence and negotiation.
ICTPA Rate Card	Approval granted by <FAS ICT SDRD>, to define the common price threshold for roles for Supplier evaluation, pricing and negotiation.
Value for Money Report	Approval granted, by <FAS ICT SDRD>, to develop the Negotiation Directive taking into consideration only those Suppliers that have met the value for money criteria detailed within the Tender Evaluation Plan.
Negotiation Directive	Approval granted, by <FAS ICT SDRD>, to commence development of individual Supplier's negotiation plans.
Negotiation Plan	Approval granted, by <FAS ICT SDRD>, to commence negotiations with Suppliers.
Negotiation Report	Approval granted, by <FAS ICT SDRD>, informs the Delegate of the outcomes of negotiations.
Section 23	Approval granted, by <FAS ICT SDRD>, to commit the expenditure of Commonwealth funds.

Table 8. Procurement Approvals and Sign-Off Descriptions

Each procurement approval is supported by input from multiple stakeholder groups.

Figure 6. Refresh Stakeholder Input RACI

Procurement Approval	Approval Authority	Associated Artefact	Responsible	Accountable	Consult	Endorse	Comment
Procurement strategy	FASICTSDR	RFT	Project Team	ICTCBS	Working Group	DICTPSG	None
Procurement Plan	FASICTSDR	Procurement Schedule	Project Team	ICTCBS	Probity	DICTPSG	None
Request for Tender	FASICTSDR	RFT	Project Team	ICTCBS	Probity	DICTPSG	None
Tender Evaluation Plan	FASICTSDR	Tender Evaluation Plan	Project Team	ICTCBS	Probity / Working Group	DICTPSG	None
Initial Screening Report	FASICTSDR	Initial Load Report	Project Team	ICTCBS	Probity	DICTPSG	None
Evaluation Report	FASICTSDR	Initial Screening Report	Project Team	ICTCBS	Probity	DICTPSG	None
ICTPA Rate Card	FASICTSDR	Initial Refresh	Project Team	ICTCBS	Working Group	DICTPSG	None
Value for Money Report	FASICTSDR	Evaluation Report TEWG Report	Project Team	ICTCBS	Probity	DICTPSG	None
Negotiation Directive	FASICTSDR	Value for Money Report	Project Team	ICTCBS	Probity	DICTPSG	None
Negotiation Plan	FASICTSDR	Negotiation Directive	Project Team	ICTCBS	Probity	DICTPSG	None
Negotiation Report	FASICTSDR	Negotiation Plan	Project Team	ICTCBS	Probity	DICTPSG	None
Section 23	FASICTSDR	All milestone artefacts	Project Team	ICTCBS	Working Group	DICTPSG	None

Figure 6. Refresh Stakeholder Input RACI

9. Risk Management

The following risks relate to the Refresh. A comprehensive Risk Register will be developed by the Program Management Office upon Refresh commencement. Refresh risks have been considered during the development of this document as follows.

Stage	Risk Description	Impact	Treatment	Likelihood
Perceived availability of non-mandatory panels				
General	Market assumption non-participating Suppliers may be easily accessed via other panels.	4	• Embed industry communications regarding Defence mandated use of ICTPA. • Consideration should be given to communication theme that acknowledge exemptions to other panels will be needed to meet Defence's needs as a matter of course and is not as an acknowledgement of ICTPA limitations.	3
Delays in decision making				
General	Introduced delays may result in: • Insufficient time to implement the scale of change planned • Postponed implementation may delay the establishment of the refreshed and future procurements under the new arrangements	5	Draft the Refresh Procurement Plan prior to endorsement to proceed to: • Ensure governance groups are aware of progression and schedule. • Tightly manage approvals to ensure steering committee engagement leading up to decision making / deliverable endorsement event.	4
Suppliers may be hesitant to participate in the Refresh process				
General	Refreshing panels is not widespread across agencies and Suppliers may not see the value in participation if they: • Have not had substantive work to date • Perceive no benefit associated with the Refresh • Do not consider participation viable due to opportunity spread outside their tier and consider the cost of participation too high.	4	Implementation of multiple touchpoints to educate Suppliers including: • Structured RFT to inform new and changed Suppliers • Supplier briefings to inform Suppliers of the progress and general ICTPA matters.	3
Resources required for the evaluation process exceed current capability/capacity				
Evaluation	Labour intensive evaluation makes it difficult secure dedicated TEWG members seeing extended evaluation, moderation and delayed conclusion.	4	• Consideration of larger number of smaller TEWGs with narrower scope to reduce evaluation duration • Consideration of surge evaluation external resources	4
Consistency of evaluation process and evaluation teams				

Figure 6. Refresh Stakeholder Input RACI

Risk Management

Stage	Risk Description	Impact	Treatment	Likelihood
Evaluation	Evaluation team scoring is inconsistent across TEWGs.	4	• Limitation of TEWG evaluation overlap • TEWG Quality Audit and reporting to support team composition-related quality issues	2
Evaluation	Inconsistent team composition, poor risk management practices at the TEWG level results in inappropriate evaluation practices and evaluator assumptions impacting overall results.	4	• On-going training and communication with TEWG leads and team members where is apparent bias is leading the evaluation process. • TEWG Quality Audit and reporting to support team composition-related quality issues	1
Perception that a discretionary refresh may not be equitable				
Evaluation	The Refresh process as initiated is perceived to have a lack of transparency, formal procedures, and improperly justified codified criteria. This may be perceived as a bias by existing panel members resulting in an erosion of confidence in ICTPA and subject to probity intervention.	2	• Suppliers entering Refresh are evaluated using equivalent criteria with similarly skilled evaluators • Communication of the Refresh Schedule confirms resources and provides a high-level description of the evaluation process and planned evaluation activity.	1
Insufficient resources to effectively engage with industry				
Engagement	Market engagement activities are scheduled for the use of the panel arrangement. Lack of Defence resources to support the associated work volumes may result in inadequate market engagement and/or loss of Supplier interest over time if their concerns are not addressed.	3	• Development of a market engagement plan with supporting timeline and work volumes to anticipate resourcing requirements for all Refresh participants.	2
Engagement	Supplier involvement during the industry engagement process must be fair and perceived to be fair by Suppliers.	3	• Industry briefing will be utilised for Supplier engagement that are open to all Suppliers. • Industry briefing will be scripted and recorded for access by any Supplier who cannot attend in person. • Industry briefing will accept pre submitted questions in the event a Supplier does not wish to ask a question live or cannot attend in person to ask the question.	1

Table 9. Refresh Risks

10. Stakeholder and Communication

The following stakeholders are impacted by the Refresh procurement. A complete stakeholder analysis will be developed as part of the Refresh once it commences. The level of impact to key stakeholders in the execution of the Refresh procurement is detailed below

Area of Impact	Level of Impact		
	Overall	Commentary	Communications Vehicle
ICT Commercial and Business Services (ICTCBS)	High	Impacts ICTCBS as a key participant in processing request documentation, and engaging industry and participating in Supplier evaluation and negotiation.	• Refresh Project Team • Working Group
Chief Technology Officer Division (CTOD)	Medium	Impact on the spectrum of services and Suppliers.	• Refresh Project Team • Working Group
NMP - CIOG	Medium	Impact on the spectrum of services and Suppliers.	• Refresh Project Team • Working Group
Chief Information Officer Group (CIOG)	Medium	Refresh has a medium resource demand on CIOG during evaluations and negotiations	• Refresh Project Team • Working Group
Extant Suppliers	Medium	Suppliers currently providing services will be required to respond to the RFT if they would like to expand their current service offering.	• Industry engagement activities
New Suppliers	Medium	Suppliers interested in the opportunity to provide services to Defence will be required to respond to the RFT and be approved to provide these services	• Industry engagement activities

Table 10. Refresh Stakeholder and Communication Plan

11. Attachment A. Probity Framework

<BI16757140> In Draft

[redacted]

Australian Government
Defence

LEGAL PROCESS AND PROBITY FRAMEWORK FOR THE ICT PROVIDER ARRANGEMENT (ICTPA) PERIODIC REFRESH

1 INTRODUCTION

1.1 Aim

1.1.1 This Framework establishes the legal process and probity principles and procedures that will apply to procurements conducted under the ICT Provider Arrangement (ICTPA) Periodic Refresh (the Project) (procurements).

1.1.2 This Framework provides the authority and structure for the way legal process and probity issues will be addressed in relation to the procurements. It establishes standards of practice and behaviour for personnel as well assigning responsibilities to individuals with specific roles in ensuring the established legal process and probity standards are met. This Framework will underpin and foster a culture of ethics and fair dealing in which documented processes are applied, a clear audit trail is established and decision making is fair, transparent and defensible.

1.1.3 In addition to the requirements of this Framework, a specific probity plan will be developed for each procurement (Probity Plan). Protocols or guidance may also be developed for particular activities where determined necessary by the Probity Manager, Probity Adviser or the Project Director. Where such protocols are developed, those protocols will form part of the Probity Plan for that procurement, and apply in addition to the other obligations under this Framework.

1.2 Background

1.2.1 The Department of Defence (Defence) introduced ICTPA on 13th July 2018 as the primary panel arrangement to source goods and services in support of its information and communications technology (ICT) environment following the expiry of the Applications Managed Services Partnership Agreement (AMSPA).

1.2.2 The 2016 Provider Arrangement Sourcing Strategy (Sourcing Strategy) recommended options to extend ICTPA in accordance with the Deed at end of years 5, 8 as well as multiple Refreshes over the term of the panel:

- if one of four predefined conditions exist (i.e. services being unavailable, demand for service not being met, value for money not being realised, or specific skills not available)

1.2.3 The 2021 ICTPA Refresh was undertaken in line with the four predefined conditions of the 2018 Panel Deed. The Refreshed Deed, executed at 30 September 2021, amended the Panel Refresh process set out in the Panel Deed to allow the Commonwealth to make changes to the structure, terms, operations and other aspects of the Panel from time to time. The ICTPA Periodic Refresh may involve undertaking a Panel Refresh from time to time in line with conditions set in the ICTPA Conditions of Deed clause 2.9 (Panel Refresh).

1.2.4 Defence has decided to extend the initial Deed Term for a period of three years in accordance with the options provided for in the Panel Deeds executed as a result of the original RFT. Accordingly, the expiry date for the existing Deed Term will be 24 June 2026. During the term of the extension it is proposed to conduct Periodic Refreshes of the panel in accordance with the Procurement Plan.

1.2.5 The proposed Periodic Panel Refresh is considered necessary to maintain currency of supplier's offerings and capture new supply markets established post previous approaches to market to meet the Commonwealth's ongoing and evolving business and military requirements.

[redacted]

1.2.6 This provides benefit by adding additional suppliers to the ICTPA through an approach to market, and allowing incumbent suppliers to expand their opportunities for service offerings.

2 AUTHORITY AND SCOPE

2.1 Authority

2.1.1 All Australian Public Service (APS) employees are bound by the standards of conduct and the obligations as stated in the APS Values and the APS Code of Conduct under the *Public Service Act 1999* (Cth) during the procurement process. In addition, Australian Defence Force (ADF) members must comply with their duties and obligations under the *Defence Force Discipline Act 1982* (Cth).

2.1.2 External Service Providers engaged to work on the procurements must comply with this Framework and note that any obligations contained in this Framework are in addition to and not in derogation of any of their contractual obligations (such as those relating to conflicts of interest).

2.2 Scope

2.2.1 Whilst the Framework is only directly applicable to those responsible for conducting the procurements, the Framework is to be provided to those members of the APS, ADF or External Service Providers working external to the procurements (including advisers, stakeholders and delegates) who are privy to sensitive information. The provision of the Framework to external personnel constitutes advice as to the behavioural standards and procedural requirements expected of personnel involved with the procurements.

2.2.2 Where appropriate, persons external to Defence who are involved in the procurements may be required to sign separate non-disclosure or confidentiality agreements where they become involved in procurement activities requiring them to have access to sensitive information.

3 GUIDELINES AND RESPONSIBILITIES

3.1 General Principles

3.1.1 All procurement activities are to be undertaken in a manner consistent with the legislative and regulatory requirements articulated in the *Public Governance, Performance and Accountability Act* (Cth) (PGPA Act), the *Commonwealth Procurement Rules* (CPRs), the Accountability Authority Instructions (AAIs) as well as key overarching policy documents, including the Defence Procurement Manual, Defence Commercial Framework, and Integrity Policy Manual.

3.1.2 Probity and ethical behaviour is one of the key principles outlined in the Commonwealth Procurement Rules. For the purposes of this Framework, probity is defined as "integrity, uprightness and honesty as exemplified in the evidence of ethical behaviour in a particular process". For more information on probity and ethics in procurement, refer to the Department of Finance website and the Integrity Policy Manual.

3.2 Process Guidelines

3.2.1 All personnel involved in the procurements must read this Framework and be aware of their obligations.

3.2.2 In adhering to this Framework the following guidelines are to be adopted:

a. for each procurement, there is to be a clear and fair procurement process that is conducted in accordance with applicable Commonwealth legislation and policy;

b. all tenderers or potential tenderers are to be treated fairly and equitably, consistent with the rules of natural justice and procedural fairness, and all interactions with tenderers or potential tenderers are to be conducted with

[redacted]

honesty, fairness and in good faith;

c. tender evaluation is to be conducted in accordance with the approved Tender Evaluation Plan;

d. commercially sensitive information is to be protected at all times and all personnel are to comply with processes established to protect and secure commercially sensitive information;

e. there must be a clear audit trail; and

f. conflicts of interest must be identified and addressed.

3.2.3 A Legal Process and Probity Checklist is provided at Annex A to help to structure arrangements and assess adherence to these guidelines.

3.3 Responsibilities of the Probity Framework Manager and Probity Manager

3.3.1 A Probity Framework Manager will be appointed to administer the Framework.

3.3.2 The responsibilities of the Probity Framework Manager will be to review this Framework with regard to probity considerations.

3.3.3 A Probity Manager will also be appointed to administer the Probity Plan for each procurement. The Probity Manager may be the same person as the Probity Framework Manager. The responsibilities of the Probity Manager in relation to that procurement will be to:

a. review all procurement process documentation with regard to probity considerations;

b. assist personnel with the identification and management of conflicts of interest, and any other potential probity issues arising in respect of the Project;

c. maintain a register of personnel who have attended a probity briefing and who have completed a conflict of interest declaration under clause 4.2;

d. maintain a register of declared conflicts of interest and steps taken to manage them;

e. assist with drafting the Tender Evaluation Plan, incorporating probity aspects where applicable; and

f. maintain a log of any communications personnel have with potential suppliers in relation to any procurement process conducted by the Project.

3.3.4 The Probity Manager will provide, or arrange for the Probity Adviser to provide, a briefing to all personnel on their responsibilities in relation to their obligations under the Probity Plan and other legal requirements where necessary (see Annex B). Any new or additional personnel will be provided with an additional briefing where necessary.

3.3.5 The Probity Framework Manager and/or the Probity Manager (as applicable) will advise the Project Director and Probity Adviser as soon as reasonably practicable if they become aware of any circumstances that suggest the Project has been, or is being, conducted in a manner inconsistent with this Framework, the relevant Probity Plan, the relevant request documentation or an approved Tender Evaluation Plan.

3.4 Responsibilities of the Probity Adviser

3.4.1 Australian Government Solicitor (AGS) has been appointed as the Probity Adviser.

3.4.2 The responsibilities of the Probity Adviser will be to advise on the conduct of the procurement, including involvement in the development and review of procurement documentation to ensure that:

a. applicable rules and procedures are followed;

b. the procurement is conducted fairly and equitably;

c. tenders received are assessed in accordance with the Tender Evaluation Plan

[redacted]

and the stated evaluation criteria; and

d. processes for managing communication with parties external to the procurements, including tenderers and potential tenderers, are established and complied with.

3.4.3 The Probity Adviser must not be involved in the evaluation, negotiation or selection of tenders as this would conflict with its role to provide unbiased and impartial advice.

3.5 Responsibilities of the Project Director

3.5.1 The Project Director is responsible for the management of, and decision making on key probity issues, including the management of any conflicts of interest in accordance with this Framework.

3.5.2 The Project Director may seek advice from the Probity Manager or Probity Adviser in relation any probity issues that arise in respect of the Project.

4 CONFLICTS OF INTEREST

4.1 Conflicts of Interest

4.1 1 A conflict of interest is where an incompatibility exists, or where it could be reasonably perceived that an incompatibility exists, between the public duty of a person and a current or prospective interest of that person or a member of that person's immediate family.

4.1.2 Instances where a conflicting interest may exist include:

a. any personal financial interest in the procurements;

b. any immediate relatives or close friends with a financial interest in the procurement;

c. any personal bias or inclination which would in any way affect an individual's decisions in relation to the procurements; or

d. any personal obligation, allegiance or loyalties that would in any way affect an individual's decisions in relation to the procurements.

4.2 Conflict of Interest Declarations

4.2.1 For each procurement, Defence personnel and a person/s engaged under a contract[1] involved in the procurement are required to sign either:

a. a Declaration of No Conflict of Interest (Annex C), which includes a declaration where no conflict of interest exists; or

b. web form AE916 to report an actual, perceived or potential conflict of interest.

Once completed, the applicable form should be submitted to the Project Director. By doing so, personnel also acknowledge that they have been briefed on this Framework, the Probity Plan, and provided with a copy of these documents and understand their contents and implications.

4.2.2 Should any actual, perceived or potential conflict of interest arise (at any stage in the procurement), Defence personnel and a person/s engaged under contract must disclose the matter through the provision of an updated conflict of interest declaration using web form AE916, which is to be submitted to the Project Director. For clarity, this may be in instances where a new actual, perceived or potential conflict of interest arises or where there is a material change to the personnel's previously declared actual, perceived or potential conflict of interest. This declaration must be provided as soon as possible after the member becomes aware that the actual, perceived or potential conflict of interest has arisen.

4.2.3 When completing the web form AE916, personnel are to:

---

[1] A person/s engaged under a contract is a contractor, consultant or outsourced service provider as defined in the Financial Delegations Glossary of Terms.

[redacted]

a. note the Project and procurement that the web form AE916 is being completed for;

b. note the list of companies of interest to the Project which will be circulated to personnel whenever the Probity Plan is distributed (or as provided by the Project Manager). The companies of interest list must be included alongside web form AE916 when it is submitted to the Project Director;

c. acknowledge that they have been briefed on this Framework and the Probity Plan, provided with a copy of these documents and understand their contents and implications; and

d. declare their actual, potential or perceived conflicts of interest in the companies of interest to the Project.

4.2.4 If at any time personnel are unsure whether they have an actual, potential or perceived conflicts of interest, personnel are to seek guidance from the Probity Manager prior to making a conflict of interest declaration.

4.2.5 A conflicts of interest register covering all personnel will be established by the Probity Manager and will be maintained to record all identified conflicts, together with all steps taken to resolve those conflicts of interest, during the conduct of the procurement process.

4.3 Management of Conflicts of Interest

4.3.1 In dealing with an actual, perceived or potential conflict of interest, AS Governance and Transformation is to act promptly as the 'decision maker' and give such directions as they see fit to address, manage or remove the conflict where it exists. Key principles for the decision maker to take into account are:

a. efforts should be made to minimise the impact on the affected person, but in all instances the interests of the Commonwealth will take precedence and may potentially lead to the restriction of access to some or all procurement related information, or the removal of the individual from the procurement.

b. during the consideration of whether a conflict of interest exists, the affected individual may be excluded from involvement in the procurement, decision or matter potentially giving rise to the conflict.

c. where an actual, potential or perceived conflict of interest is deemed by the decision maker to exist, the decision maker may exclude the effected individual from involvement in the procurement, decision or matter.

d. individuals affected by any such determination are not to provide advice, inform the decision making process, make decisions or exercise any concurrence or delegation in relation to the procurement, decision or matter in question.

e. where, after consideration, the decision maker determines that no actual or potential conflict exists, the details of the matter and the findings of the decision-maker are to be recorded. Generally no further action need be taken.

f. for the purposes of deciding on the existence of a conflict of interest, the issue is not whether the person has actually been influenced, but whether a reasonable person would perceive that the decision making process of an individual could have been influenced. Consequently, where a perceived conflict of interest exists, the decision maker is to make such determinations that place the probity of the procurement, including the way the procurement is perceived, as paramount.

4.4 Acceptance of Gifts and Hospitality

4.4.1 The solicitation or acceptance of gifts or hospitality from any party that has a likely or potential interest or association with the procurements, including prospective tenderers, is prohibited. Should personnel involved in the procurements consider that exceptional circumstances exist that warrant a variation to this blanket policy, they

[redacted]

are to seek the written approval of Project Director who will consider the request in accordance with the Integrity Policy Manual and Financial Policy Gifts and Benefits, and any other relevant Defence policy.

4.5 Offers of Employment

4.5.1 In accordance with the Defence Instruction Administrative Policy Annex C – AG5 – Conflicts of Interest and Declarations of Interest, the Integrity Policy Manual and Defence Commercial Framework, personnel involved in the procurements who receive an offer of post separation employment from a potential tenderer, tenderer, or contractor (whether or not the offer of employment is in writing), and is considering that offer of employment, must immediately advise Project Director in writing.

4.6 Communication with Tenderers or Potential Tenderers

General

4.6.1 As part of treating all tenderers and potential tenderers fairly and equitably and consistently with the rules of procedural fairness and natural justice, personnel involved in the procurements must not communicate with the tenderers or potential tenderers in a manner which:

a. gives, or gives rise to the perception of, an unfair advantage to that tenderer or potential tenderer;

b. reveals proprietary or confidential information of another tenderer or potential tenderer; or

c. unfairly disadvantages a tenderer or potential tenderer.

Business as usual activities

4.6.2 Personnel should be aware that one or more of the current suppliers on the ICTPA panel may wish to submit a tender under the procurement processes. While business as usual contact with current suppliers will need to continue, personnel should ensure that their dealings with current suppliers do not give rise to any actual or perceived unfair advantage to those suppliers under the procurement processes. Personnel dealing with current suppliers on business as usual matters in the lead up to and during the procurement process must comply with the protocols in Annex D.

5 CONFIDENTIAL INFORMATION

5.1 Scope of Confidential Information

5.1.1 'Confidential Information' means information (whether or not provided by the Commonwealth) that meets all of the following criteria:

a. is specifically identified;

b. is commercially sensitive (i.e. the information should not generally be known or ascertainable);

c. disclosure would cause unreasonable detriment to the owner of the information or another party (e.g. disclosure of a contractor's profit margin); and

d. was provided with an expressed or implied understanding that it would remain confidential,

but does not include information that:

e. is or becomes public knowledge other than by breach of contract or obligation of confidentiality; or

f. is in the possession of a party without restriction in relation to disclosure before the date of receipt.

5.2 Management of Confidential Information

5.2.1 Personnel involved in the procurement should only have access to Confidential

[redacted]

Information on an appropriate 'need to know' basis. Confidential Information needs to be managed in accordance with the information's commercial sensitivity and/or classification level.

5.2.2 All personnel involved in the procurements who may be privy to Confidential Information are obliged to ensure that all such information remains confidential and is not disclosed to anyone other than other personnel who require such disclosure in order to perform their duties for the procurement.

5.2.3 Personnel having access to Confidential Information must ensure that documents and information, including electronically stored information, that is in their possession or control and which contains Confidential Information is:

a. kept in locked offices or locked filing cabinets when not in use;

b. not left unattended for any period at a place that is accessible by a person not authorised;

c. not displayed at times or in places where they could be read by a person who is not authorised;

d. not made available to a person who is not authorised; and

e. password protected (in the case of electronically stored material).

6 EXPIRY

6.1 Survivorship

6.1.1 Unless expressly, or by implication from its nature, intended to survive the expiry of the Framework, the requirements of this Framework will expire at the conclusion of the Refresh activities or as otherwise determined by the Project Director.

s22

[redacted]

s47E(d)

Director ICTPSG

Service Delivery and Reform

CIOG

16 February 2023

Annexes:

A. Legal Process and Probity Checklist
B. Probity Briefing Template
C. Declaration of No Conflict of Interest

[redacted]

ANNEX A: LEGAL PROCESS AND PROBITY CHECKLIST

PROBITY PLANNING

Determine whether a probity auditor and/or adviser is needed	☐
Obtain Declaration of No Conflicts of Interest or confirm personnel have completed Conflict of Interest Declaration AE916 for any actual, potential or perceived conflict of interest	☐
Obtain confidentiality agreements from external participants	☐
Finalise the Legal Process and Probity Framework and Probity Plan, if one is being used	☐
Consider confidentiality requirements	☐
Set up physical security procedures, such as the document register or data room	☐
Ensure team members are familiar with all relevant policies and documents	☐
Set up procedures so all potential suppliers have access to the same information	☐

PROCUREMENT PROCESS

Review probity at the end of the request documentation preparation process	☐
Document any changes that occur to the request documentation, and notify all potential tenderers	☐
Establish procedure for opening of tenders (including use of local tender rooms)	☐
Set up a process for receiving, recording and acknowledging or clarifying tenders	☐
Ensure evaluation of submissions is fair and consistent with the evaluation plan	☐
Review probity at the end of the evaluation process	☐
Notify the successful tenderer as soon as possible	☐
Notify the unsuccessful tenderers as soon as possible	☐
Debrief unsuccessful tenderers	☐
Ensure all actions are documented, and the documents are stored appropriately	☐
Review probity at the end of the process	☐

ANNEX B: DRAFT PROBITY BRIEFING

Refer to the Probity Briefing Template.

[redacted]

ANNEX C: DECLARATION OF NO CONFLICT OF INTEREST FOR ICT PROVIDER ARRANGEMENT (ICTPA) ROLLING REFRESH (THE PROJECT)

I declare that:

(a) I have read and understood the Legal Process and Probity Framework and the Probity Plan (Plan) for the Project, and acknowledge that it is my responsibility to comply with the Framework and the Plan;

(b) I have no actual, perceived or potential conflicts of interest, as defined in the Framework, which would conflict with my role in the Project; and

(c) if an actual, perceived or potential conflict of interest arises, I will immediately provide an updated declaration (via web form Conflict of Interest Declaration AE916) to the Project Director in accordance with the requirements of the Framework.

Details of Signatory	
Signature:	
Printed Name:	
Rank/Level/Title:	
Appointment/Organisation:	
Phone/email Contact:	
Date:	

Return to the Probity Manager: [insert details].

[redacted]

ANNEX D: BUSINESS AS USUAL PROTOCOLS

1 PROBITY PROTOCOLS

1.1.1 Personnel who have contact with tenderers or potential tenderers outside of the procurement process must adhere to the following protocols:

a. discussions with tenderers or potential tenderers should be limited to day to day business as usual matters arising under the ICTPA and should not include any matters relating to the procurement process;

b. information about the procurement process must not be discussed with, or disclosed to, tenderers or potential tenderers outside of the procurement process – in particular, personnel must not, outside of the process:

(i) provide any information relating to the procurement process to a tenderer or potential tenderer or any other person who does not have a need to know;

(ii) disclose information about the evaluation of a response to a tenderer or any other person who does not have a need to know; or

(iii) discuss the procurement process in public spaces where those discussions could be overheard by tenderers or potential tenderers or any other person who does not have a need to know;

c. where meetings or discussions are held with current suppliers or any other potential tenderers, personnel should, where appropriate, confirm that the discussion does not form part of, and does not relate to, the procurement process, which personnel are unable to discuss for probity reasons;

d. where a tenderer or potential tenderer seeks to discuss the procurement process other than through the nominated contact officer, personnel must:

(i) decline to comment;

(ii) refer the enquiry to the Project Director;

(iii) make a record of that contact and how it was handled; and

(iv) provide that record to the Probity Manager;

e. personnel must not:

(i) coach any tenderer or potential tenderer in relation to their response to the procurement process; or

(ii) express, directly or indirectly, any views or opinions regarding the procurement process, including about the evaluation process or a tenderer's or potential tenderer's proposed or actual approach, chances of success, or capacity to perform;

f. personnel must not provide potential tenderers with an opportunity to comment on, or contribute to, the development of any of the procurement documentation outside of the procurement process;

g. where appropriate, personnel should ensure that if any substantive discussions or meetings are held with tenderers or potential tenderers in the lead up to or during the procurement process:

(i) records are maintained;

(ii) at least two Defence personnel are in attendance; and

(iii) they are not held in public places;

h. where personnel have substantial contact with a tenderer or potential tenderer as part of business as usual activities, they should consider keeping records of those business as usual activities in the lead up to and during the procurement process (as evidence that the procurement was not discussed);

[redacted]

and

i. where personnel are involved in the procurement process, personnel must:

(i) comply with all of the requirements of the Probity Plan, including those in relation to gifts, hospitality and offers of employment; and

(ii) in completing any conflict of interest declaration, declare their business as usual activities with tenderers or potential tenderers.

2 CO-LOCATED PERSONNEL

2.1.1 Some potential tenderer personnel may be co-located with Defence personnel in order to perform services under the current ICTPA or other contracts. Defence personnel working in locations where potential tenderer personnel are present (**Co-located Personnel**) will need to continue to engage with potential tenderer personnel in the lead up to and during the procurement process.

In addition to the protocols in section 1 above, Co-located Personnel should ensure that confidential information about the procurement process is not accessed while in co-located areas or, where this is not possible, take steps to ensure such information is protected at all times from access by potential tenderer personnel. For example:

a. information about the procurement process must not be able to be viewed by potential tenderer personnel (e.g. on screens in an open plan environment);

b. information about the procurement process must not be left unattended on desks, printers or photocopiers; and

c. information about the procurement process must be stored securely when not in use (e.g. through the use of screen locks and lockable containers).

[redacted]

Prepared for the Department of Defence
s47E(d) Director Strategic Commercial Management–ICTPA/FSG
Your ref: s47E(d) Our ref: 20204047
15 February 2023

Probity sign-off – Periodic Refresh Procurement Plan

1. AGS is engaged as probity adviser for Defence's ICT Provider Arrangement (ICTPA) Standing Offer Panel Refresh, which includes the Periodic Refresh process.

2. Defence has prepared a Procurement Plan for the Periodic Refresh process (Procurement Plan).

3. The Procurement Plan provides for a series of procurements to refresh the panel by adding suppliers to ICTPA and allowing existing suppliers to expand the scope of the services they are able to provide under the ICTPA.

4. This sign-off opinion relates to the Procurement Plan provided to us for probity review on 14 February 2023.

Probity sign-off

5. Subject to the assumptions set out in paragraph 6, in our view, the Procurement Plan does not, to the best of our knowledge, give rise to any material legal process or probity risks that have not been brought to Defence's attention.

Assumptions

6. This probity sign-off is subject to the following assumptions:

   a. we have assumed that the Procurement Plan has not been, and will not be, substantively changed from the version provided to us (except to the extent required to address any of our comments or suggested changes)

   b. we have relied on the accuracy and completeness of all information provided to us

   c. we have assumed, and have no reason not to believe, that Defence has raised any material probity matters relevant to the Procurement Plan with us

   d. noting that further approvals will be required for each new procurement conducted in accordance with the Procurement Plan, we have assumed that Defence has complied with, or will comply with, all its internal procedures and requirements for the approval of the Procurement Plan.

7. This probity sign-off is provided solely for the benefit of Defence and we acknowledge that Defence will rely on it. This sign-off may not be provided to, or relied upon by, any other person without AGS consent. This sign-off is strictly limited to the matters stated in it and does not apply by implication to any other matters.

[redacted]

[redacted]

Contact

s22 [redacted]

Stuart Hilton
Senior Executive Lawyer
T s47E(d) [redacted]
s47E(d) [redacted]@ags.gov.au

[redacted]

Australian Government

Department of Defence

ENTERPRISE PROCESS OWNER – PEOPLE

EPO-P 101.1

PMKeyS Information System - Security Practices and Procedures (IS-SPP)

Version 4.3

(intentionally left blank)

REVISION HISTORY

Author	Organisation	Date	Version	Comment
s47E(d)	DPS	1 AUG 2005	1.6	Changes from ISA review for OHSC.
	PCSC	12 SEP 2005	1.6.1	Amendments.
	DPS	12 JAN 2006	1.6.2	Clarification of user access requirements.
	PCSC	31 JAN 2006	1.6.3	Update document – Roles of ISSO & Security Manager
	DPS	15 FEB 2006	1.6.4	Updated comments from PCSC.
	DPCSC	10 MAR 2006	1.6.5	Updated comments
	DPS	23 MAR 2006	2	Updated to include PCSC comments.
	DPS	28 NOV 2006	2.1	Update to reflect restructure.
	DPCSC	20 AUG 2008	2.2	Review and update
	DPCSC	NOV 2010	2.3	Review and update
	ADSCG	AUG 2014	3.0	Review and update to reflect new Privacy laws
	AD S&G, PSBS	NOV 2017	3.1	Review and update
	PSBS SPARA	DEC 2017	3.2	Review and update
	AD S&G, PSBS	DEC 2017	3.3	Review and update
	AD S&G, PSBS	SEP 2019	4.0	Minor updates, incremented for authorisation.
	PSBS SPARA	NOV 2019	4.1	Review and update
	PSBS SPARA	FEB 2020	4.2	Review and update
	PSBS SPARA	MAY 2020	4.2	Review and update
	PSBS SPARA	AUG 2020	4.3	Change password length from ten to 14 characters

AUTHORISATION

Document Authoriser	Version	Signature
Director People Systems Business Support	v4.3	s22 5/8/20

Proposals for amendment, or requests for copies of this Documentation Control Standard, are to be forwarded to:

Assistant Director S&G (CP1-7-035)
s47E(d)
Department of Defence
CANBERRA ACT 2600

TABLE OF CONTENTS

DEFINITION OF TERMS

[redacted] – the Application has a system security rating of [redacted] where:

a. The highest classification of information processed on PMKeyS is [redacted];

b. Access to an associated workstation is restricted to users with a minimum security clearance of Baseline as outlined in the Protective Security Policy Framework (PSPF); and

c. Access to PMKeyS is restricted to users who have a 'Need-to-Know' requirement for the data and have been granted formal approval.

Workstation – the term 'Workstation' refers not only to the computer unit but to any storage and production media used in conjunction with the unit. This includes remote logon via DREAMS and the Home Portal; and media such as removable drives such as USB Flash drive, separate printers and other storage devices.

PMKeyS – the term "PMKeyS includes the PMKeyS Portal, Business Application, and Self Service. The term extends to Customer Relations Management (CRM) applications, including ComTrack Self Service, which are accessed via the PMKeyS Portal. Where aspects of this document relate to the PMKeyS Business Application only, the relevant paragraphs will include the words 'PMKeyS Business Application. In all other cases this IS-SPP applies to the entire PMKeyS suite.

PMKeyS Data – the term 'PMKeyS Data refers to data accessed directly through the PMKeyS application and/or sourced from PMKeyS reports, extracts, and interfaces. The term also refers to data that is available through other applications that are automatically or manually loaded with data sourced from PMKeyS.

Human Resource Reporting Applications – this document does not specifically cover the access management arrangements for Human Resource Reporting Applications, including MARS, HRMeS and InfoSphere, however the Goals and Objectives of this IS-SPP apply to the Human Resource Reporting Applications. For details on the access management practices and procedures for the Human Resource Reporting Applications refer to the MARS Website.

PART ONE – GENERAL INFORMATION

Introduction

1. ICT Security concerns the control of data. Security measures are implemented to ensure that data is stored, processed, transferred, and is adequately protected according to its sensitivity. The PMKeyS Security Operating Procedures, known as the PMKeyS Information System - Security Practices and Procedures (IS-SPPs), are designed for a system security rating of [redacted] and apply to the entire PMKeyS suite.

2. PMKeyS is hosted on the Defence Protected Network (DPN) and is accessible directly via the DPN, through a DREAMS logon to the DPN, the Home Portal, and through the deployable networks. This IS-SPP does not replace the CIOG Defence Secret Network and Defence Protected Network System User Acceptable Usage Standard Operating Procedure (accessible via the PMKeyS Portal page) and which outlines the responsibilities of all users that access the DPN.

Document Relationships

3. This IS-SPP is referenced to the Australian Government Information Security Manual (ISM), the Protective Security Policy Framework (PSPF), the Defence Security Principles Framework (DSPF), and the Australian Privacy Principles (APPs) as stated in the *Privacy Act 1988*.

4. Detailed instructions on the management of access to PMKeyS are provided on the PMKeyS – Access & Password webpage.

Audience

5. This IS-SPP is to be read prior to all users being granted access to the PMKeyS Business Application and/or the CRM Applications. It is a requirement that the IS-SPP is read and acknowledged by all users of PMKeyS.

Goals

6. The goals of this IS-SPP are to:

   a. Establish a standard set of security policy practices and procedures to be used by all users of PMKeyS;

   b. Reduce the risk of information loss by accidental or intentional disclosure, destruction or denial of access;

   c. Maintain the security, privacy, integrity and availability of PMKeyS; and

   d. Ensure all personnel with access to PMKeyS take responsibility for the data they manage and/or use.

Objectives

7. To meet these goals, the following objectives must be achieved:

   a. Prevention of unauthorised access, disclosure, modification, manipulation, or deletion of PMKeyS data;

   b. Authentication of PMKeyS users;

   c. Establishment of security mechanisms that are flexible and responsive to changes in organisational structures and individual responsibilities;

d. Provision of means for identifying unauthorised access to PMKeyS and/or data and for taking appropriate corrective, preventative or disciplinary action;

e. Limit the use of PMKeyS to the purposes for which such resources are intended;

f. Ensure appropriate governance is in place for the security and privacy protection of PMKeyS data when accessed through applications and databases other than PMKeyS; and

g. Ensure that the system sponsor and/or delegates and authorised users are aware of their respective responsibilities with regards to maintaining the security of the data.

Scope

8. This is a 'living' document and its contents will be constantly monitored to ensure it is up-to-date and relevant.

9. The practices and procedures contained in this document are to apply to all data created, processed, and stored on PMKeyS.

PART TWO – PRACTICES AND PROCEDURES

General

10. PMKeyS has a security rating of [redacted]. All users must be cleared to Baseline and have a 'Need-to-Know' requirement for data to which formal access has been approved. Depending upon the level of access requested, users wishing to access data for Protected Identities must have a minimum security clearance of Negative Vetting 1.

Conditions of Access

11. Before gaining access to the PMKeyS Business Application and/or the CRM application, personnel must:

a. Read and understand this IS-SPP.

b. Be aware of their responsibilities in using PMKeyS, as detailed in paragraphs 22 – 27 below.

c. Be granted as a minimum, a security clearance equal to the classification of Baseline. Higher security clearances are required for some levels of PMKeyS access.

d. Have a 'Need-to-Know' requirement to access the data for the purpose of performing assigned tasks.

e. Have been appropriately trained for the required PMKeyS access, and are competent to browse and/or transact in PMKeyS. Have completed the Campus courses mandatory for PMKeyS access; *Australian Privacy Principles eAssessment* and *Defence One Introduction & Reporting*. To gain access to the Global Payroll application, the *Defence One Introduction to Global Payroll* Campus course must also be completed.

f. Request PMKeyS Access via Self Service. This access request method is available to users where their Service or Group has mapped PMKeyS access roles to positions, and where the user has completed the prerequisite PMKeyS training courses. In cases where the PMKeyS roles to position have not been mapped, or access is requested for a CRM application, the user and supervisor are to complete Webform *AD688 Application for Defence One Access* form.

12. **Supervisors** are to ensure that personnel using the Webform AD688:

a. Applied for the appropriate access required to perform their assigned tasks;

b. Met mandatory training requirements for the access requested; and

c. Read and understood this IS-SPP.

13. **Special Authorisation** is required before access can be granted to sensitive data including, but not limited to, Career Management, Discipline, Human Resource Budgeting, Drugs and Alcohol and Professional Development & Training. Additional detail is provided at paragraphs 30 – 31, below.

Password Management

14. Access to the Portal is given to all ADF and APS personnel upon commencement. Access to the Portal is only given to Contractors where access to the PMKeyS Business Application has been authorised.

15. PMKeyS identifies individual users by their unique Operator ID and password. For APS and ADF users, the Operator ID is the user's Employee ID. For Contractors, the Operator ID is the user's Other Defence Staff (ODS) number (date of birth & initials), preceded by the letter C.

16. Users must change their password during their initial login. The password protects the user's account from unauthorised use. Passwords are classified as Official: Sensitive and must not be revealed to any other person.

17. The following policies are to be enforced by PMKeyS on all user passwords:

a. Users are forced to change passwords every 90 days on the Portal for continued access to PMKeyS, Self Service and CRM;

b. Passwords must be a minimum of 14 alpha/numeric characters long and should contain at least three of the following character sets

(1) Lowercase alphabetic characters (a-z)

(2) Uppercase alphabetic characters (A-Z)

(3) Numeric characters (0-9)

(4) Special characters ((! @ # $ % ^ & * ( ) - _ = + \ | [ ] { } ; : / ? . , > <)

c. The same password cannot be used in any 30 password rotation; and

d. Users will be locked out after three successive failed logon attempts.

18. The PMKeyS Information Technology Security Officer (ITSO) is to be notified if a user's password is compromised, or suspected of being compromised. The PMKeyS ITSO is to log the details and initiate action for the compromised password to be changed.

19. Automated procedures for deletion of access to PMKeyS are documented on the PMKeyS website. Refer to the Access Purge Process on the Privacy & Security webpage.

20. The PMKeyS ITSO is responsible for monitoring and auditing the issuing of Operator IDs and passwords to authorised users. For a full description of the duties of the ITSO, see Annex A.

21. Users are required to set up their PMKeyS Portal password reset hint on initial login. Users who have forgotten their password (and have not set up a reset hint) or have a locked account are to contact the Defence Service Centre (DSC) for assistance. Refer to the Password Management webpage.

User Responsibilities

22. All users must:

a. Abide by the policies, practices and procedures set out in this document; and

b. Report at once any attempted or actual breach of security to the PMKeyS ITSO via email s47E(d)

23. All users are responsible for:

a. Maintaining the **confidentiality** and **integrity** of information stored on PMKeyS; and

b. Reading and understanding the PMKeyS IS-SPP prior to granting of access to the PMKeyS Business Application and/or CRM, or when notified that amendments have been made.

24. Supervisors are responsible for ensuring that the user has read, understood and complies with the PMKeyS IS-SPP.

25. No user is to attempt to bypass or defeat the security systems, or attempt to obtain use of passwords or privileges issued to another person.

26. All users are to use their account only, and to only use their account for specific work related tasks. Unauthorised changes to or creation of PMKeyS accounts are not to be made and will be investigated as a breach.

27. All users, prior to being given access to PMKeyS, shall be made aware of their responsibilities and shall complete a declaration that they accept the above responsibilities. By signing an AD688 Application for Defence One Access form, or by accepting the *Privacy & Security Acknowledgement* when applying for PMKeyS access via Self Service, the user signifies that they have read, understood, and accept the terms and conditions set out in this PMKeyS IS-SPP.

Privileged Users

28. The administration of PMKeyS permits certain users to hold accounts that enable a greater level of functionality than is offered by a standard user account. This includes maintenance personnel, security personnel, system administrators, database administrators and users granted Privileged access as defined by the Australian Government Information Security Manual (ISM). Those with Privileged access have the same responsibilities under the IS-SPP as a standard user.

29. Privileged user access will be reviewed monthly for compliance confirmation by the SPARA team within People Systems Business Support and/or their delegates. An access review can be conducted at any time by the user themselves, or the user's supervisor/manager.

Privileged users are required to maintain a correction log as documented in the Auditing Requirements webpage. The PMKeyS ITSO and/or their delegates/Business areas may conduct regular audits of correction logs to ensure compliance.

30. Special Authorisers are in place to ensure that personnel requesting access to PMKeyS have:

a. Requested the appropriate privileged access to adequately perform their assigned tasks;

b. Undertaken the required PMKeyS training and are competent to transact in PMKeyS;

c. Read and understood the PMKeyS IS-SPP; and

d. Understand the Australian Privacy Principles and how they apply to PMKeyS.

31. Special Authorisers are to ensure they are aware of their respective responsibilities and the responsibilities of the users they are authorising with regard to maintaining the security and privacy of information.

System Security Sponsor

32. The System Security Sponsor (Director PSBS), and/or their delegates are responsible for the following:

a. Reviewing the PMKeyS IS-SPP to ensure that it continues to comply with the goals and objectives detailed in Part One (General Information) of this document;

b. Ensuring the implementation of, and sustained compliance with, the PMKeyS IS-SPP;

c. Resolving information system security issues in consultation with the PMKeyS ITSO;

d. Ensuring an ITSO is nominated for the PMKeyS application;

e. Ensuring that the ITSO and Security Manager carry out their duties in accordance with Annex A of this document; and

f. Ensuring that the current version of the IS-SPP is available for viewing by all users on PMKeyS via the Portal logon page, and on the PMKeyS website.

Access to PMKeyS Sourced Data through other Applications or Databases

33. PMKeyS data can be provided routinely or adhoc to other Defence and non-Defence applications and databases via interface or extract. To ensure appropriate security and privacy protection of the PMKeyS sourced data, the owners of the other applications and databases are to put in place Data Management Agreements (DMA) and procedures that adhere to Part One of this IS-SPP.

34. The Directorate of Workforce Information (DWI) is to ensure that a DMA is completed before PMKeyS data is provided to other Defence and non-Defence applications and databases. The DWI is to ensure that the DMA is distributed and endorsed by other data owners such as the Director of PSBS and the other system owner(s) as the recipients of the data.

35. For applications and databases outside Defence, DWI is to ensure that a Data Management Agreement is completed before PMKeyS data is provided to these non-Defence applications and databases.

36. For Defence applications and databases being provided with PMKeyS data through a PMKeyS batch process, PSBS is responsible for ensuring appropriate security management is applied. This is required before PSBS signs off the System Change Request, Functional Specification, and User Acceptance Testing.

37. For Defence applications and databases being provided with PMKeyS data through a DWI provided extract, DWI is responsible for ensuring appropriate security management is applied.

Breaches of Security

38. All breaches of security are to be reported and investigated in accordance with the standards contained in ISM and DSPF. Any attempted or actual breach of PMKeyS security is to be reported to the PMKeyS ITSO via email s47E(d)

39. Any user who has access to a Defence/Defence Industry domain or inter-domain connection will be in breach of security if they:

a. Attempt to access information and/or resources without the required authorisation, clearance, and/or briefing;

b. Attempt to access information and/or resources, and cannot justify their need for access;

c. Attempt to circumvent the access mechanisms that have been applied to protect information and/or resources;

d. Attempt to deny functionality of the system to any other person without prior authorisation;

e. Attempt to corrupt information that may be of value to Defence;

f. Do not take reasonable steps to confirm that the information that they originate will be protected;

g. Extract information from the system and pass it to a person who does not have an established 'Need-to-Know' requirement, or is not authorised to access that information;

h. Attempt to modify information and/or resources without authority; and

i. Process information that is classified above the level allowed.

40. The personal information contained within PMKeyS is subject to the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988*. The APPs provide legal direction on the collection, storage, use and disclosure of sensitive and personal data. Please refer to the Defence Privacy website for further information.

41. Intended, unauthorised, or inappropriate use or disclosure of personal information contained within PMKeyS is an infringement of the *Privacy Act 1988*. It is also a breach of the *Public Service Act 1999* Part 3, Section 13 (the APS Code of Conduct), and the *Defence Force Discipline Act 1982*. Such breaches may result in corrective action taken under the relevant provisions of the *Defence Force Discipline Act 1982*, or the *APS Code of Conduct Procedures*. Actions may include:

a. A reprimand;

b. Removal from part or all of the PMKeyS application;

c. Reduction in salary by way of a monetary fine;

d. Reduction in classification;

e. Termination of service with the Department of Defence; and

f. Civil charges.

ANNEX A

Duties of the PMKeyS Information Technology Security Officer (ITSO)

1. The PMKeyS Information Technology Security Officer is the PMKeyS Security Policy, Audit, and Requirements Analysis (SPARA) Team Leader within People Systems Business Support (PSBS). The PMKeyS ITSO is responsible to the System Sponsor and/or delegate for the following:

a. Perform administration in support of PMKeyS security and the application of Defence security policy and standards;

b. Develop and implement PMKeyS security policy in consultation with PMKeyS stakeholders;

c. Ensuring procedures are in place to grant the appropriate PMKeyS access to personnel based upon the business authorised roles to be performed by the users requesting access;

d. Maintain and monthly audit a list of all 'Privileged Users';

e. Review and contribute to the relevant PMKeyS security training;

f. Provide an escalation path to enable personnel to bring to notice all suspicious incidents;

g. Maintain a register of reported fraudulent and security breach incidents and forward to relevant identified authority as required; and

h. Act as the liaison between system personnel and assist in identifying and correcting security deficiencies.

Note: A Deputy PMKeyS ITSO, the SPARA APS 5, has been appointed and is able to perform all of the PMKeyS ITSO duties mentioned above in the absence of the Team Leader, Security Policy, Audit and Requirements Analysis (SPARA) ITSO.

Duties of the PMKeyS Information Technology Security Manager (ITSM)

1. The PMKeyS Information Technology Security Manager is the PSBS Assistant Director of Security and Governance (AD S&G) and is responsible for the following aspects of the system management in relation to security:

a. Management of PMKeyS security policy.

b. Standards compliance is maintained in accordance with the ISM, DSPF and the *Privacy Act 1988.*

2. The PMKeyS Information Technology Security Manager is **not** to be the PMKeyS ITSO.

From: s47E(d)
To: s47E(d)
Subject: FW: DSOC - D1TU PMKeyS Security Assessment - Final Report [SEC=
Date: Friday, 11 March 2022 11:10:00 AM

s47E(d)

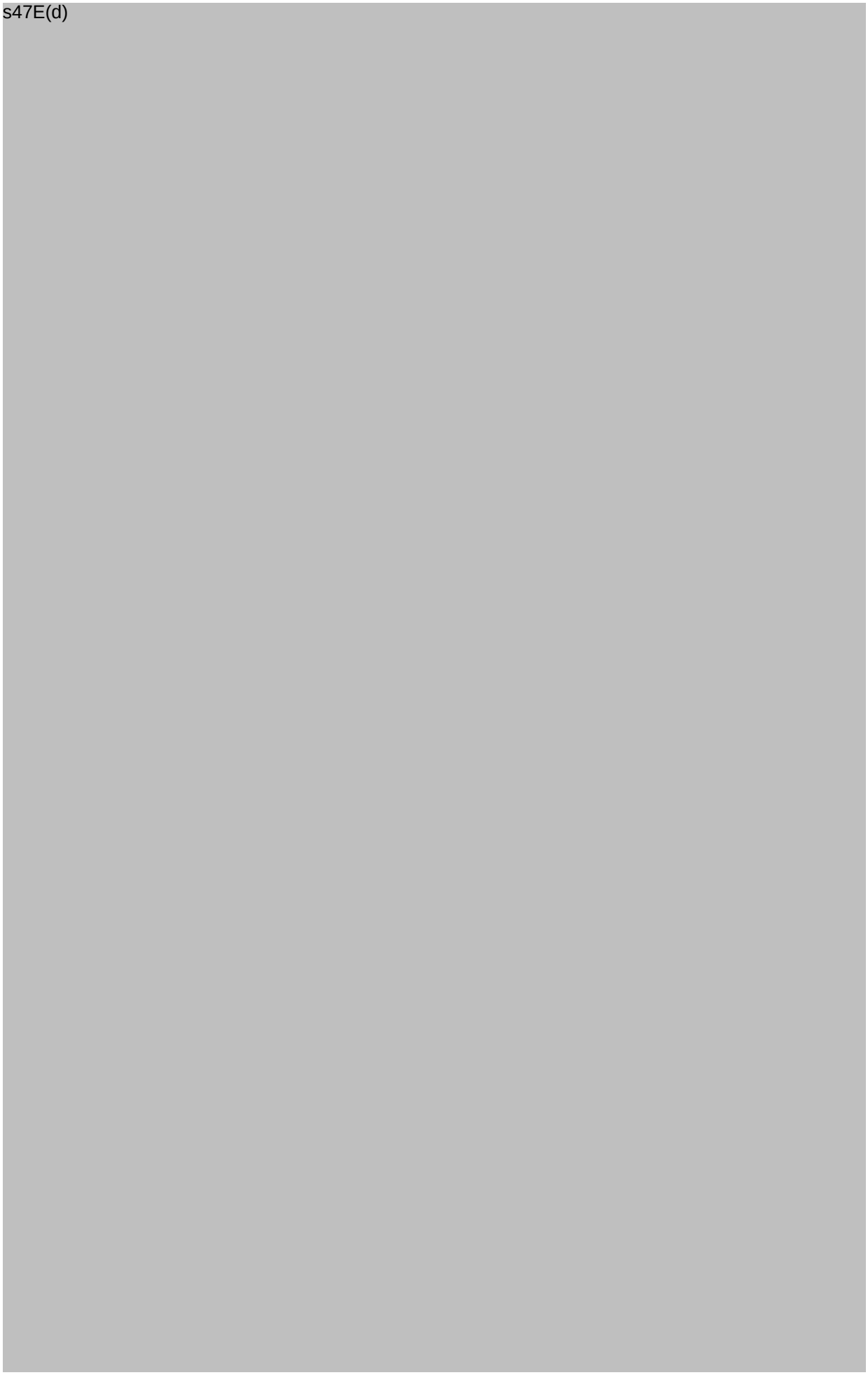
As discussed here is the summary of actions …

All rows highlighted AMBER needs support from other teams to resolve the issue and rows GREEN are actioned or will be actioned soon.

Please let me know if more information is required.

s47E(d)

s47E(d)



Thanks
s47E(d)

From: s47E(d)
Sent: Thursday, 3 March 2022 10:29 AM
To: s47E(d)
Cc: s47E(d)
s47E(d)
Subject: RE: DSOC - D1TU PMKeyS Security Assessment - Final Report [SEC=

Good Morning s47E(d)

My apologies for not responding to you earlier with the remediation plan in response to findings published. s47E(d) and we are currently in the closure state and expect final closure by end-March 22.

All the findings in s47E(d) s47E(d) and as a consolidated response the Remediation Action Plan for each of the findings has been provided (see attachment).

As the project is winding up the remediation plan will be actioned by CIOG/HICTO/ETOB/DPSS.

Please let me know if additional information or details are required.

Kind Regards,

s47E(d)

ICT People Domain Delivery
Corporate & Logistics Delivery Branch | ICT Delivery Division
Chief Information Officer Group | Department of Defence
s47E(d) | ACT
M: s22
E: s47E(d)
Chat: Lync Instant Messaging

From: s47E(d)
Sent: Monday, 24 May 2021 3:17 PM
To: s47E(d)
s47E(d)
Cc: s47E(d)
s47E(d)
Subject: DSOC - D1TU PMKeyS Security Assessment - Final Report [SEC=

Good Afternoon,

DSOC has produced the final Security Assessment report for the Defence One Technical Upgrade project's PMKeyS Application, see attached.

Kind Regards,

---

s47E(d)
Team Lead – Cyber Readiness Team C – Assessments
Defence Security Operations Centre
ICT Security Branch | ICT Operations Division
Chief Information Officer Group | Department of Defence

s47E(d) | Canberra ACT
P: s47E(d) E: s47E(d)

"High Performance, Teamwork and Respect"

From: s47E(d)
To: s47E(d)
Cc: s47E(d)
Subject: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC=
Date: Monday, 19 September 2022 5:24:00 PM
Attachments: image001.jpg
image002.png
image003.jpg
PMKeyS Privacy & Security - Final.obr
Privacy Statement Jul 2015.obr

Hey Team

s22

From my understanding on the below request from DWI, our Privacy Statement requires an update.
I've attached two links 1) PMKeyS Privacy & Security and 2) Privacy Statement.
I think it is the Privacy Statement that needs to be reviewed but I'm happy to be corrected.

Happy to discuss, if required.

Kind Regards

s47E(d)
Director
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610
P: s47E(d) | E: s47E(d) @defence.gov.au

From: s47E(d) @defence.gov.au>
Sent: Thursday, 1 September 2022 2:42 PM
To: s47E(d) @defence.gov.au>
Subject: FW: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement

[redacted]

Hi s47E(d)

s47E(d) has noted a good point below but before I go back to her, I have a question or two that you might have answers two:

- Is there anywhere else I can find Information Privacy Principles, as currently my belief is the reference is to the Privacy Policy which no longer refers to this
- The current privacy principles *(May 2021)* does not have a Section 14 which is referred to in our '2007 Privacy Framework', stupid question but is there more than one?

My belief is that the Privacy Framework could almost been complete re-written however, I would rather double check the information.

Kind regards,

s47E(d)
A/Assistant Director
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Defence Plaza Melbourne | 661 Bourke Street | Melbourne | VIC 3000
P: s47E(d)

From: s47E(d) @defence.gov.au>
Sent: Monday, 1 August 2022 5:19 PM
To: s47E(d) @defence.gov.au>
Subject: FW: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC= [redacted]

[redacted]

Hi

I thought I'd have a quick look at this. Before I continue, when you get a spare minute, can you please have a quick look at the Privacy Act 1988 and just let me know if you can even find the references made in this draft?

I can't even see where anything refers to "IPP" (only APP) nor the 11 principles in Section 14. While the intent of the document is understandable, I just can't confirm where they got their information from and this draft has 2007 on it?.....The current Act as per the legislation register has recently been updated.

s22 I'm willing to re-do a lot but just need to confirm if I AM supposed to be referencing the Privacy Act 1988 / Defence Privacy Policy (attached).

Regards

s47E(d)
Security Policy, Audit & Requirements Analysis (SPARA)
People Systems Business Support
People Systems and Payroll Services Branch
Department of Defence
PH: s47E(d)

Want more information on PMKeyS Security and Access? Visit the PMKeyS Security Access & Passwords site.

I acknowledge the traditional owners of country. I pay my respect to the Worimi peoples of Port Stephens, their culture and to the elders; past, present and emerging.

From: s47E(d)
Sent: Monday, 1 August 2022 11:47 AM
To: s47E(d)
Subject: FW: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC [redacted]

[redacted]

Hi s47E(d),

I'll discuss this with you, in our catch up ☺

You most likely won't be able to access the original (OBJ).

Kind regards,

s47E(d)
A/Assistant Director
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Defence Plaza Melbourne | 661 Bourke Street | Melbourne | VIC 3000
P: s47E(d)

From: s47E(d) @defence.gov.au>
Sent: Friday, 29 July 2022 2:28 PM
To: s47E(d) @defence.gov.au>
Subject: RE: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC

Hi s47E(d),
Great to have a chat with you.

As I promised, please check my comments (After page 24) in attached file for your considerations.
For you awareness, s47E(d) will be the next right person as POC as IPM Team Lead for further coordination in future.

s22

Cheers.

Kind Regards,
s47E(d)

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

From: s47E(d) @defence.gov.au>
Sent: Monday, 18 July 2022 10:51 AM
To: s47E(d) @defence.gov.au>
Cc: s47E(d) @defence.gov.au>
Subject: FW: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC=

Hi s47E(d),

Can I please ask where this Privacy Statement is? s47E(d) and I are unable to access the link.

Kind regards,

s47E(d)
Team Leader
PMKeyS Security Policy. Audit & Requirement Analysis (SPARA)
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Defence Plaza Melbourne | 661 Bourke Street | Melbourne | VIC 3000
P: s47E(d)

From: s47E(d) @defence.gov.au>
Sent: Monday, 18 July 2022 10:33 AM
To: s47E(d) @defence.gov.au>
Subject: RE: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC=

Hi s47E(d),

I did not aware s47E(d) has mentioned to update in PIA. As you see, I have not been address on the email at first place.

I would not be able to open your attached objective link as I do not have the access.

However, s47E(d) and I have updated IS-SPP couple of weeks ago (End of June) in attachment for your awareness.

Let me know if you need anything from me for PIA.

Kind Regards,

s47E(d)
Team Leader
Innovation & Project Management
Security and Governance
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610
P: s47E(d) | E: s47E(d) @defence.gov.au

-

From: s47E(d) @defence.gov.au>
Sent: Monday, 18 July 2022 9:06 AM
To: s47E(d) @defence.gov.au>
Subject: FW: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC=

Hi s47E(d),

Is this still in progress on your end? This was left for me to action and s47E(d) said she herself, hadn't started it?

Kind regards,

s47E(d)
Team Leader
PMKeyS Security Policy. Audit & Requirement Analysis (SPARA)
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Defence Plaza Melbourne | 661 Bourke Street | Melbourne | VIC 3000
P: s47E(d)

From: s47E(d) @defence.gov.au>
Sent: Monday, 16 May 2022 11:15 AM
To: s47E(d)
Subject: [TASK 001/22]- PIA Recommendations to update PMKeyS Privacy Statement [SEC=

Hi s47E(d)

Can you please take the lead in updating the PMKeyS Privacy Statement and please collaborate with s47E(d).

s22

Kind Regards

s47E(d)
Assistant Director - Security and Governance
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610

P: s47E(d) | E: s47E(d) @defence.gov.au

From: s47E(d) @defence.gov.au>
Sent: Friday, 7 January 2022 2:42 PM
To: s47E(d) @defence.gov.au>
Cc: s47E(d) @defence.gov.au>
Subject: FW: DIS - PIA Recommendations to update PMKeyS Privacy Statement
[SEC=

Hi s47E(d)
Apologies for the delay.

Hi s47E(d),
s22 noting that we need to update the PMKeyS Privacy Statement... noting also the staffing situation in SPARA. Let's discuss.

Cheers

s47E(d)

s47E(d)
Director
Directorate of People Systems Business Support
People Systems & Payroll Services Branch
Defence People Group

s47E(d) | Campbell Park Offices | PO Box 7909 | Canberra BC | ACT 2610
P: s47E(d) | M: s22

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

From: s47E(d) @defence.gov.au>
Sent: Thursday, 18 November 2021 4:12 PM
To: s47E(d) @defence.gov.au>
Cc: HRIM s47E(d) @defence.gov.au>
Subject: DIS - PIA Recommendations to update PMKeyS Privacy Statement
[SEC=

Hi s47E(d),

Thank you for the chat yesterday.

As discussed, please see attached the DPG WHS Defence Interim Solution (DIS) draft PIA, which includes recommendations that have been raised by DPG WHS to update the PMKeyS Privacy Statement that also applies to the HR data housed in the DWI HRDW.

Summary of risks and recommendations related to PMKeyS Privacy Statement is located on page 61 of this document, recommendations numbered 10,11,12.

I am aware of Defence Privacy (s47E(d)) previously engaging with your business area to update the PMKeyS Privacy Statement but not sure how far this progressed. s47E(d) has now moved on and the new POC in Defence Privacy is s47E(d) .

If you can let us know who you allocate this task to that would be much appreciated.

Kind regards,

s47E(d)

HR Domain – Information Management (HRIM)
Directorate of Workforce Information (DWI)
Workforce Planning Branch
Department of Defence

s47E(d) | Canberra Airport | PO Box 7922 | Canberra BC | ACT 2610
P: s47E(d)

PMKeyS Privacy and Security

Privacy

Privacy is protected by law In Australia through the *Privacy Act 1988* (the Privacy Act). The Privacy Act outlines the required protection of personal information in certain circumstances and sets out how agencies, such as Defence, need to handle personal information.

PMKeyS holds HR and payroll related information for all Defence employees. This personal information is subject to the Australian Privacy Principles (APPs) as set out in the Privacy Act which means that the unauthorised use or disclosure of personal information contained in personal records is a breach of the APPs. All personnel with access to or receive data from PMKeyS need to know that the APPs apply to them.

Specifically, APP6 outlines when an APP entity (ie an organisation subject to the APPs – which includes all Australian Government agencies) may use or disclose personal information. Generally that use or disclosure must be in regard to the reason the information was originally collected.

APP11 relates to the security of personal information and requires Defence to take reasonable steps to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Click on the following link for further details on the Privacy Act and the APPs.
http://www.oaic.gov.au/privacy-law/ .

Access, Use and Disclosure of Personal Information

Before getting access to or receiving data from PMKeyS, all users agree to adhere to the Privacy Act, and Information System-Security Practices and Procedures.Users also need to do the APPs eAssessment (course ID#7392) before they will be given access. Each time users log into or request data from PMKeyS they will need to acknowledge that they will abide by the APPs.

Unauthorised use or disclosure of personal information is a breach of the APPs and the ISSPPs. All personnel are reminded that the APS Code of Conduct (APS employees), or the *Defence Force Discipline Act 1982* (DFDA) (ADF members) apply to their actions.

Personnel with Protected Identity Status

Access to information in PMKeyS is strictly controlled and should only be given to authorised users who have a authorised need to access it. Access to information about people with a Protected Identity status (as specified in Defence Security Principles Framework - Control 42.1) has additional requirements.

> The special controls around access to and release of information relating to Protected Identities are set out under the Defence Security Principles Framework – Control 42.1. Personnel authorised to access personal information of these personnel must consult this reference beforehand.

Notification of Data Breaches

The Notifiable Data Breaches Scheme under the Privacy Act requires Defence to notify the Office of the Australian Information Commissioner about 'eligible data breaches'. Further Information about the Notifiable Data Breach Scheme can be found at the following link:
http://drnet/People/Privacy/Pages/Privacy-Data-Breaches.aspx

Further Information

For further information on Privacy in Defence please refer to the Defence Privacy website: http://drnet/People/Privacy/Pages/Privacy.aspx or contact the Defence Privacy Office via defence.privacy@defence.gov.au.

For further information on Privacy and Security in Defence One/PMKeyS please refer to the Defence One website: http://drnet.defence.gov.au/People/PMKeyS/Access-and-Password/Pages/PMKeyS-Privacy-and-Security.aspx or contact the Defence One Security Policy via s47E(d) .

Privacy and Security of personal information in Defence is everybody's responsibility.

From: s47E(d)
To: s47E(d)
Subject: [SIGNED]-[FINAL APPROVAL] IS-SPP 2022 [SEC=OFFICIAL]
Date: Wednesday, 7 December 2022 6:04:00 PM
Attachments: image001.png
image002.jpg
image003.png
IS SPP 2022 - DEC 2022.pdf
IS SPP 2022 - DEC 2022.docx

OFFICIAL

Hi s47E(d)

I have made minor amendments and have attached both the Word and PDF signed versions. We will need to update our webpage – Resources section with the new updated version, including the Home Portal link to IS-SPP.
Would you also mind sending a copy to HRIM s47E(d) @defence.gov.au / s47E(d) and other regular stakeholders.

Thank you so much, kicking goals!!!!

Kind Regards

s47E(d)
Director
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610
P: s47E(d) | E: s47E(d) @defence.gov.au

From: s47E(d) @defence.gov.au>
Sent: Wednesday, 7 December 2022 9:46 AM
To: s47E(d) @defence.gov.au>
Subject: [FINAL APPROVAL] IS-SPP 2022 [SEC=OFFICIAL]

OFFICIAL

Hi s47E(d),

If you are happy with the attached, I will convert it to PDF for you to sign.

Kind regards,

s47E(d)
A/Assistant Director
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

DPM-9 | Defence Plaza Melbourne | 661 Bourke Street | Melbourne | VIC 3000
P: s47E(d)

From: s47E(d) @defence.gov.au>
Sent: Wednesday, 7 December 2022 9:03 AM
To: s47E(d) @defence.gov.au>
Cc: s47E(d) @defence.gov.au>
Subject: Completed: IS-SPP 2022 - For your signature [SEC=OFFICIAL]

OFFICIAL

Morning s47E(d),

Please see attached completely updated IS SPP document.

If you are happy with this please sign the authorisation field on page iv.

Once you've signed it, I'll release it.
Just to clarify, in order to release it I must:

a. Save it correctly in OBJ
b. Talk to s47E(d) (SPARA) to update the websites
c. Contact CIOG to update the PMKeyS sign on link

Let me know.

Kind Regards,

s47E(d)
Team Leader
PMKeyS Access Management
PSBS Security & Governance
People Systems Business Support (PSBS)

People Systems and Payroll Services (PS&PS)
Department of Defence

s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610
P: s47E(d) | E: s47E(d) @defence.gov.au

s22

From: s47E(d) @defence.gov.au>
Sent: Wednesday, 30 November 2022 12:49 PM
To: s47E(d) @defence.gov.au>
Subject:]FOR ACTION] IS-SPP 2022 [SEC=OFFICIAL]

OFFICIAL

Hi s47E(d),

I have managed to source the information from CIOG and have provide further updates internal to the document.

In addition to this, I have also fixed up the formatting however, you'll need to run your eyes over it and accept tracked changes.

Once this is complete, we should be able to release this version – Excellent work on this, thank you!

Kind regards,

s47E(d)
A/Assistant Director
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence

s47E(d) | Defence Plaza Melbourne | 661 Bourke Street | Melbourne | VIC 3000
P: s47E(d)

From: s47E(d) @defence.gov.au>
Sent: Saturday, 19 November 2022 2:55 PM
To: s47E(d) @defence.gov.au>
Cc: s47E(d) @defence.gov.au>
Subject: [FOR ACTION - REVIEW - ADVICE] - IS-SPP 2022 [SEC=OFFICIAL]

OFFICIAL

Hi s47E(d),

Please find attached updated IS-SPP.

I have reviewed your comments & responded, could you please consider the additional changes/information.

Also, may I please ask for your advice on the formatting.

Happy to call and chat about it on Monday, hope you are having a lovely weekend.

Kind Regards,

s47E(d)
Team Leader
PMKeyS Access Management
PSBS Security & Governance
People Systems Business Support (PSBS)
People Systems and Payroll Services (PS&PS)
Department of Defence

s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610
P: s47E(d) | E: s47E(d) @defence.gov.au

s22

From: s47E(d) @defence.gov.au>
Sent: Friday, 18 November 2022 2:06 PM
To: s47E(d) @defence.gov.au>
Subject: RE: [FOR ACTION] - Review & Provide Feedback on IS SPP 2022 - [DUE] - Friday 7 October [SEC=OFFICIAL]

OFFICIAL

Hi s47E(d),

I have just had a look at the attached, I have also added some comments.

If required, feel free to liaise with s47E(d) or myself to finalise the changes in this document ☺

Regards,

s47
E(d)

From: s47E(d) @defence.gov.au>
Sent: Monday, 31 October 2022 1:34 PM
To: s47E(d) @defence.gov.au>
Subject: FW: [FOR ACTION] - Review & Provide Feedback on IS SPP 2022 - [DUE] - Friday 7 October [SEC=OFFICIAL]

OFFICIAL

Hi s47E(d)

As discussed.

Kind Regards,

s47E(d)
A/Team Leader
PMKeyS Security Policy
PSBS Security & Governance
People Systems Business Support (PSBS)
People Systems and Payroll Services (PS&PS)
Department of Defence

s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610
P: s47E(d) | E: s47D @defence.gov.au

From: s47E(d) @defence.gov.au> **On Behalf Of** HRIM
Sent: Wednesday, 5 October 2022 11:30 AM
To: s47E(d) @defence.gov.au>; @defence.gov.au>
Subject: RE: [FOR ACTION] - Review & Provide Feedback on IS SPP 2022 - [DUE] - Friday 7 October [SEC=OFFICIAL]

OFFICIAL

Hi s47E(d),

Thank you for the opportunity to review the IS SSP doc.

Looks good, only the 1 suggested inclusion – see comment. It is with regards to including a statement of requirement for a system wanting to consume HR data.

Let me know if you have any questions.

Thanks,
s47E(d)
a/assistant Director
HR Domain – Information Management

HR Information Management (HRIM)
Directorate Workforce Information (DWI)
Workforce Planning (WP)
Defence People Group
s47E(d) | Brindabella Park | PO Box 7927 | Canberra BC| ACT 2610
P: s47E(d) |

From: s47E(d) @defence.gov.au>
Sent: Wednesday, 28 September 2022 8:55 AM
To: HRIM <hr.infomanagement@defence.gov.au>
Cc: s47E(d) @defence.gov.au>
Subject: [FOR ACTION] - Review & Provide Feedback on IS SPP 2022 - [DUE] - Friday 7 October [SEC=OFFICIAL]

OFFICIAL

Good morning HRIM team,

I have recently edited the IS SSP document to ensure it is current, could you please assist by reviewing & providing feedback on the attached.

Please provide your input by **COB Friday 7 October.**

Please let me know if you require any assistance or have any questions.

Thank you for your help,

Kind Regards,

s47E(d)
A/Assistant Director
Security & Governance
People Systems Business Support (PSBS)
People Systems and Payroll Services Branch
Department of Defence
s47E(d) | Campbell Park Offices | PO Box 7909 | ACT 2610
P: s47E(d) | M: s22 | E: s47E(d) @defence.gov.au

Australian Government

Defence

ENTERPRISE PROCESS OWNER – PEOPLE

EPO-P 101.1

PMKeyS Information System - Security Practices and Procedures (IS-SPP)

Version 4.5

(intentionally left blank)

REVISION HISTORY

Author	Organisation	Date	Version	Comment
s47E(d)	DPS	1 AUG 2005	1.6	Changes from ISA review for OHSC.
s47E(d)	PCSC	12 SEP 2005	1.6.1	Amendments.
s47E(d) / s47E(d)	DPS	12 JAN 2006	1.6.2	Clarification of user access requirements.
s47E(d)	PCSC	31 JAN 2006	1.6.3	Update document – Roles of ISSO & Security Manager
s47E(d)	DPS	15 FEB 2006	1.6.4	Updated comments from PCSC.
s47E(d)	DPCSC	10 MAR 2006	1.6.5	Updated comments
s47E(d)	DPS	23 MAR 2006	2	Updated to include PCSC comments.
s47E(d)	DPS	28 NOV 2006	2.1	Update to reflect restructure.
s47E(d)	DPCSC	20 AUG 2008	2.2	Review and update
s47E(d)	DPCSC	NOV 2010	2.3	Review and update
s47E(d)	ADSCG	AUG 2014	3.0	Review and update to reflect new Privacy laws
s47E(d)	AD S&G, PSBS	NOV 2017	3.1	Review and update
s47E(d)	PSBS SPARA	DEC 2017	3.2	Review and update
s47E(d)	AD S&G, PSBS	DEC 2017	3.3	Review and update
s47E(d)	AD S&G, PSBS	SEP 2019	4.0	Minor updates, incremented for authorisation.
s47E(d)	PSBS SPARA	NOV 2019	4.1	Review and update
s47E(d)	PSBS SPARA	FEB 2020	4.2	Review and update
s47E(d)	PSBS SPARA	MAY 2020	4.2	Review and update
s47E(d)	PSBS SPARA	AUG 2020	4.3	Change password length from ten to 14 characters
s47E(d)	PSBS	SEP 2022	4.4	Update password character requirements, access to PI data obligations
s47E(d)	PSBS	DEC 2022	4.5	Review and update

AUTHORISATION

Document Authoriser	Version	Signature
Director People Systems Business Support	v4.5	

Proposals for amendment, or requests for copies of this Documentation Control Standard, are to be forwarded to:

Assistant Director S&G
s47E(d)
Department of Defence
CANBERRA ACT 2600

TABLE OF CONTENTS

DEFINITION OF TERMS

[redacted] – the Application has a system security rating of ~~PROTECTED~~ where:

a. The highest classification of information processed on Personnel Management Key Solution (PMKeyS) is [redacted]

b. Access to an associated workstation is restricted to users with a minimum security clearance of Baseline as outlined in the Protective Security Policy Framework (PSPF); and

c. Access to PMKeyS is restricted to users who have a genuine 'need-to-know' requirement to view ~~PROTECTED~~ data and have been granted formal approval.

Workstation – the term 'Workstation' refers not only to a computer unit (including Defence Protective Laptop) but to any storage and production media used in conjunction with a unit. This includes remote logon via DREAMS, the Home portal and media such as; removable drives for example USB Flash drives, separate printers and other storage devices.

PMKeyS – the term 'PMKeyS' includes the PMKeyS portal, Business Application, and Self Service. The term extends to Customer Relations Management (CRM) applications, including ComTrack Self Service (CSS), which are accessed via the PMKeyS Portal. Where aspects of this document relate to the PMKeyS Business Application only, the relevant paragraphs will include the words 'PMKeyS Business Application'. In all other cases this IS-SPP applies to the entire PMKeyS suite.

PMKeyS Data – the term 'PMKeyS Data' refers to data accessed directly through the PMKeyS application and/or sourced from PMKeyS reports, extracts and interfaces. The term also refers to data that is available through other applications that are automatically or manually loaded with data sourced from PMKeyS.

Human Resource Reporting Applications – this document does not specifically cover the access management arrangements for Human Resource Reporting Applications, including Management and Analysis Reporting Solution (MARS), Human Resource Metric System (HRMeS) and a data integration platform named InfoSphere; the Goals and Objectives of this IS-SPP apply to the Human Resource Reporting Applications. For details on access management practices and procedures for the Human Resource Reporting Applications, refer to the MARS Website.

PART ONE – GENERAL INFORMATION

Introduction

1. ICT Security in the context of PMKeyS concerns the control of data in PMKeyS. Security measures are implemented to ensure that data is stored, processed, transferred, and is adequately protected according to its sensitivity. The PMKeyS Security Operating Procedures, known as the PMKeyS Information System - Security Practices and Procedures (IS-SPP), are designed for a system security rating of [redacted] and apply to the entire PMKeyS software suite.

2. PMKeyS is hosted on the Defence Protected Network (DPN) and is accessible directly via the DPN (including via Defence Protected laptops), through a DREAMS logon to the DPN, the Home portal, and through the deployable networks. PMKeyS is hosted on the Defence Protected Network (DPN) and is accessible directly via the DPN (including via Defence Protected laptops), through a DREAMS logon to the DPN, the Home portal, and through the deployable networks. This IS-SPP does not replace the Defence Security Principles Framework (DSPF), that outlines the responsibilities of all users' access to the DPN.Document Relationships

3. This IS-SPP is referenced to the Australian Government Information Security Manual (ISM), the Protective Security Policy Framework (PSPF), the Defence Security Principles Framework (DSPF), and the Australian Privacy Principles (APPs) as stated in the *Privacy Act 1988*.

4. Detailed instructions on the management of access to PMKeyS are provided on the PMKeyS – Access & Password webpage.

Audience

5. This IS-SPP is to be read prior to all users being granted access to the PMKeyS Business Application and/or the CRM and/or CSS Applications. It is a requirement that the IS-SPP is read and acknowledged by all users of PMKeyS.

Goals

6. The goals of this IS-SPP are to:

   a. Establish a standard set of security policy practices and procedures to be used by all users of PMKeyS;

   b. Reduce the risk of information loss by accidental or intentional disclosure, destruction or denial of access;

   c. Maintain the security, privacy, integrity and availability of PMKeyS and the data held in PMKeyS; and

   d. Ensure all personnel with access to PMKeyS take responsibility for the data they manage and/or use.

Objectives

7. To meet these goals, the following objectives must be achieved:

   a. Prevention of unauthorised access, disclosure, modification, manipulation, or deletion of PMKeyS data;

   b. Authentication of PMKeyS users;

   c. Establishment of security mechanisms that are flexible and responsive to changes in organisational structures and individual responsibilities;

d. Provision of means for identifying unauthorised access to PMKeyS and/or data and for taking appropriate corrective, preventative or disciplinary action;

e. Limit the use of PMKeyS to the purposes for which such resources are intended;

f. Ensure appropriate governance is in place for the security and privacy protection of PMKeyS data when accessed through applications and databases other than PMKeyS; and

g. Ensure that the system sponsor and/or delegates and authorised users are aware of their respective responsibilities with regards to maintaining the security of the data.

Scope

8. This is a 'living' document and its contents will be constantly monitored to ensure it is up-to-date and relevant.

9. The practices and procedures contained in this document are to apply to all data created, processed, and stored on PMKeyS.

PART TWO – PRACTICES AND PROCEDURES

General

10. PMKeyS has a security rating of [redacted] All users must be cleared to Baseline and have a 'Need-to-Know' requirement for data to which formal access has been approved. Depending upon the level of access requested, users requiring access to data for Protected Identities must have a minimum security clearance of Negative Vetting 1.

Conditions of Access

11. Before gaining access to the PMKeyS Business Application and/or the CRM application, personnel must:

a. Read and understand this IS-SPP.

b. Be aware of their responsibilities in using PMKeyS, as detailed in paragraphs 22 – 27 below.

c. Be granted as a minimum, a security clearance equal to the classification of Baseline. Higher security clearances are required for some levels of PMKeyS access.

d. Have a 'Need-to-Know' requirement to access the data for the purpose of performing assigned tasks.

e. Have been appropriately trained for the required PMKeyS access, and are competent to browse and/or transact in PMKeyS. Have completed the Campus courses mandatory for PMKeyS access; *Australian Privacy Principles eAssessment* and *Defence One Introduction & Reporting*. To gain access to the Global Payroll application, the *Defence One Introduction to Global Payroll* Campus course must also be completed.

f. Request PMKeyS Access via Self Service. This access request method is available to users where their Service or Group has mapped PMKeyS access roles to positions, and where the user has completed the prerequisite PMKeyS training courses. In cases where the PMKeyS roles to position have not been mapped, or access is requested for a CRM application, the user and supervisor are to complete Webform *AD688 Application for PMKeyS Access* form.

g. Access to Protected Identity data can only be granted with the agreement of the relevant Protected Identity authorisers.

12. **Supervisors** are to ensure that personnel using the Webform AD688:

a. Applied for the appropriate access required to perform their assigned tasks;

b. Met mandatory training requirements for the access requested; and

c. Read and understood this IS-SPP.

13. **Special Authorisation** is required before access can be granted to sensitive data including, but not limited to; Career Management, Discipline, Human Resource Budgeting, Drugs and Alcohol and Professional Development & Training. Additional detail is provided at paragraphs 32 – 33 below.

Password Management

14. Access to the PMKeyS portal is given to all ADF and APS personnel upon commencement. Access to the PMKeyS portal is only given to contractors where access to the PMKeyS Business Application has been authorised.

15. PMKeyS identifies individual users by their unique Operator ID and password. For APS and ADF users, the Operator ID is the user's Employee ID. For contractors, the Operator ID is the user's Other Defence Support (ODS) number (date of birth & initials), preceded by the letter C.

16. Users must change their password during their initial login. The password protects the user's account from unauthorised use. Passwords are classified as 'Official: Sensitive' and must not be revealed to any other person.

17. The following policies are to be enforced by PMKeyS on all user passwords:

a. Users are forced to change passwords every 90 days on the PMKeyS Portal for continued access to PMKeyS, Self Service and CRM;

b. Passwords must be a minimum of fourteen (14) characters in length and a maximum of thirty two (32) characters consisting of the following character sets:

(1) Lowercase alphabetic characters (a-z)

(2) Uppercase alphabetic characters (A-Z)

(3) Numeric characters (0-9)

(4) Special characters (! @ # $ % ^ & * ( ) - _ = + \ | { } [ ]; : ? / . ,)

c. The same password cannot be used in any 30-day password rotation; and

d. Users will be locked out after three consecutive failed logon attempts.

18. The PMKeyS Information Technology Security Officer (ITSO) is to be notified if a user's password is compromised, or suspected of being compromised. The PMKeyS ITSO is to log the details and initiate action for the compromised password to be changed.

19. Automated procedures for deletion of access to PMKeyS are documented on the PMKeyS website. Refer to the Access Purge Process on the Privacy & Security webpage.

20. The PMKeyS ITSO is responsible for monitoring and auditing the issuing of Operator IDs and passwords to authorised users. For a full description of the duties of the ITSO, refer to Annex A.

21. Users are required to set up their PMKeyS Portal password reset hint on initial login. Users who have forgotten their password (and have not set up a reset hint) or have a locked account are to contact the Defence Service Network (DSN) for assistance. Refer to the Password Management webpage.

User Responsibilities

22. All users must:

a. Abide by the policies, practices and procedures set out in this document; and

b. Report at once any attempted or actual breach of security to the PMKeyS ITSO via email s47E(d) ; and/or

c. Report any shared or suspected PI data spills by completing an XP188 form

23. It is the responsibility of all users to:

a. Maintain **confidentiality** and **integrity** of information stored on PMKeyS; and

b. Read and understand the PMKeyS IS-SPP prior to granting access to the PMKeyS , CRM and/or CSS Business Applications, or when notified that amendments have been made.

24. Supervisors are responsible for ensuring that a user has read, understood and complies with the PMKeyS IS-SPP.

25. No user is to attempt to bypass or defeat the security systems, or attempt to obtain use of passwords or privileges issued to another person.

26. All users must use their own account for specific work-related tasks only. Unauthorised changes to, or creation of, PMKeyS accounts is not permitted .Any suspected changes will be investigated as a breach.

27. Prior to granting access to PMKeyS, all users are to be made aware of their responsibilities and complete a declaration as acceptance of responsibilities. By signing an AD688 Application for PMKeyS Access form, or by accepting the *Privacy & Security Acknowledgement* when applying for PMKeyS access via Self Service, the user acknowledges they have read, understood, and accept the terms and conditions set out in this PMKeyS IS-SPP.

Privileged Users

28. The administration of PMKeyS permits certain users to hold accounts that enable a greater level of functionality than is offered by a standard user account. This includes maintenance personnel, security personnel, system administrators, database administrators and users granted privileged access as defined by the ISM. Those with privileged access have the same responsibilities under the IS-SPP as a standard user.

29. In accordance with ICT Security advice, privileged access accounts cannot be used via DREAMS or a Defence Protected Laptop. Privileged accounts can only be accessed on computers in secure Defence establishments using the Defence Protected Network.

30. Privileged user access are reviewed quarterly for compliance confirmation by the Security Policy Audit Requirements Analysis (SPARA) team in People Systems Business Support (PSBS) and/or their delegates. An access review can be conducted at any time by the user themselves, or the user's supervisor/manager.

31. Privileged users are required to maintain a correction log as documented in the Requirements webpage. The PMKeyS ITSO and/or their delegates/Business areas may conduct regular audits of correction logs to ensure compliance.

32. Special Authorisers are in place to ensure that personnel requesting access to PMKeyS have:

a. Requested the appropriate privileged access to adequately perform their assigned tasks;

b. Undertaken the required PMKeyS training and are competent to transact in PMKeyS;

c. Read and understood the PMKeyS IS-SPP; and

d. Understand the Australian Privacy Principles and how they apply to PMKeyS.

33. Special Authorisers are to ensure they are aware of their respective responsibilities and the responsibilities of the users they are authorising with regard to maintaining the security and privacy of information.

System Security Sponsor

34. The System Security Sponsor (Director PSBS) and/or their delegates are responsible for:

a. Conducting a review of the PMKeyS IS-SPP to ensure it continues to comply with the goals and objectives detailed in Part One (General Information) of this document;

b. Ensuring the implementation of, and sustained compliance by running monthly and quarterly reports, and engaging with customer to justify their requirement for accessing PMKeyS and meeting their obligations for security, the PMKeyS IS-SPP;

c. Resolving information system security issues in consultation with the PMKeyS ITSO;

d. Ensuring an ITSO is nominated for the PMKeyS application;

e. Ensuring that the ITSO and Security Manager carry out their duties in accordance with Annex A of this document; and

f. Ensuring that the current version of the IS-SPP is available for viewing by all users on PMKeyS via the Portal logon page, and on the PMKeyS website.

Access to PMKeyS Sourced Data through other Applications or Databases

35. PMKeyS data can be provided routinely or adhoc to other Defence and non-Defence applications and databases via interface or extract. To ensure appropriate security and privacy protection of the PMKeyS sourced data the following needs to occur before data will be provided:

a. any application or database that will store PMKeyS data must undertake analyse from CIOGs ICTSB team and be accredited as reliable and trustworthy.

b. the owners of the other applications and databases are to put in place Data Management Agreements (DMA) and procedures that adhere to Part One of this IS-SPP.

36. The Directorate of Workforce Information (DWI) is to ensure that a DMA is completed before PMKeyS data is provided to other Defence and non-Defence applications and databases. The DWI is to ensure that the DMA is distributed and endorsed by other data owners such as the Director of PSBS and the other system owner(s) as the recipients of the data.

37. For applications and databases outside Defence, DWI is to ensure that a DMA is completed before PMKeyS data is provided to these non-Defence applications and databases.

38. For Defence applications and databases being provided with PMKeyS data through a PMKeyS batch process, PSBS is responsible for ensuring appropriate security management is applied. This is required before PSBS signs off the System Change Request, Functional Specification, and User Acceptance Testing.

39. For Defence applications and databases being provided with PMKeyS data through a DWI provided extract, DWI is responsible for ensuring appropriate security management is applied.

Breaches of Security

40. All breaches of security are to be reported and investigated in accordance with the standards contained in ISM and DSPF. Any attempted or actual breach of PMKeyS security is to be reported to the PMKeyS ITSO via email s47E(d) .

41. Any user who has access to a Defence/Defence Industry domain or inter-domain connection will be in breach of security if they:

a. Attempt to access information and/or resources without the required authorisation, clearance, and/or briefing;

b. Attempt to access information and/or resources, and cannot justify their need for access;

c. Attempt to circumvent the access mechanisms that have been applied to protect information and/or resources;

d. Attempt to deny functionality of the system to any other person without prior authorisation;

e. Attempt to corrupt information that may be of value to Defence;

f. Do not take reasonable steps to confirm that the information that they originate will be protected;

g. Extract information from the system and pass it to a person who does not have an established ‘Need-to-Know’ requirement, or is not authorised to access that information;

h. Attempt to modify information and/or resources without authority; and

i. Process information that is classified above the level allowed.

42. The personal information contained within PMKeyS is subject to the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988*. The APPs provide legal direction on the collection, storage, use and disclosure of sensitive and personal data. Please refer to the Defence Privacy website for further information.

43. Intended, unauthorised, or inappropriate use or disclosure of personal information contained within PMKeyS is an infringement of the *Privacy Act 1988*. It is also a breach of the *Public Service Act 1999* Part 3, Section 13 (the APS Code of Conduct), and the *Defence Force Discipline Act 1982*. Such breaches may result in corrective action taken under the relevant provisions of the *Defence Force Discipline Act 1982*, or the *APS Code of Conduct Procedures*. Actions may include:

a. A reprimand;

b. Removal from part or all of the PMKeyS application;

c. Reduction in salary by way of a monetary fine;

d. Reduction in classification;

e. Termination of service with the Department of Defence; and

f. Civil charges.

ANNEX A

Duties of the PMKeyS Information Technology Security Officer (ITSO)

1. The PMKeyS Information Technology Security Officer is the PMKeyS Security Policy, Audit, and Requirements Analysis (SPARA) Team Leader within People Systems Business Support (PSBS). The PMKeyS ITSO is responsible to the System Security Sponsor and/or delegate for the following:

a. Perform administration in support of PMKeyS security and the application of Defence security policy and standards;

(1) Specifically analysing reports, queries or any extracts containing PMKeyS data including sensitive information, particularly for Users who have row security. (Access to view PI data)

b. Develop and implement PMKeyS security policy in consultation with PMKeyS stakeholders, and communicate with PMKeyS users;

(1) To exercise caution and be aware that reports will produce PI data unless configured to exclude PI units. (Please exclude PI Units' data when running reports, where there is no requirement for PI data output)

(2) That to share PI data is considered a breach or data spill, as this data cannot be viewed without appropriate PI authorisation

c. Ensuring procedures are in place to grant the appropriate PMKeyS access to personnel based upon the business authorised roles to be performed by the users requesting access

d. Perform and analyse quarterly audits of all listed 'Privileged Users'

e. Review and contribute to the relevant PMKeyS security training

f. Provide an escalation path to enable personnel to bring notice to all suspicious incidents, including;

(1) Investigations of all attempted or actual breaches of security; and

(2) Investigations of all attempted or actual data spills reported via XP188 forms

g. Prioritise the investigation of any attempted or actual data spills and implement risk management and policy changes to prevent these incidents re-occurring

h. Maintain a register of reported fraudulent and security breach incidents and forward to relevant identified authority as required; and

i. Act as the liaison between system personnel and assist in identifying and correcting security deficiencies.

Note: A Deputy PMKeyS ITSO, the SPARA APS 5, has been appointed and is able to perform all of the PMKeyS ITSO duties mentioned above in the absence of the Team Leader SPARA ITSO.

Duties of the PMKeyS Information Technology Security Manager (ITSM)

1. The PMKeyS Information Technology Security Manager is the PSBS Assistant Director of Security and Governance (AD S&G) and is responsible for the following aspects of the system management in relation to security:

a. Management of PMKeyS security policy.

b. Standards compliance is maintained in accordance with the ISM, DSPF and the *Privacy Act 1988*.

2. The PMKeyS Information Technology Security Manager is **not** to be the PMKeyS ITSO.

Australian Government

Defence

ENTERPRISE PROCESS OWNER – PEOPLE

EPO-P 101.1

PMKeyS Information System - Security Practices and Procedures (IS-SPP)

Version 4.5

(intentionally left blank)

REVISION HISTORY

Author	Organisation	Date	Version	Comment
s47E(d)	DPS	1 AUG 2005	1.6	Changes from ISA review for OHSC.
s47E(d)	PCSC	12 SEP 2005	1.6.1	Amendments.
s47E(d) / s47E(d)	DPS	12 JAN 2006	1.6.2	Clarification of user access requirements.
s47E(d)	PCSC	31 JAN 2006	1.6.3	Update document – Roles of ISSO & Security Manager
s47E(d)	DPS	15 FEB 2006	1.6.4	Updated comments from PCSC.
s47E(d)	DPCSC	10 MAR 2006	1.6.5	Updated comments
s47E(d)	DPS	23 MAR 2006	2	Updated to include PCSC comments.
s47E(d)	DPS	28 NOV 2006	2.1	Update to reflect restructure.
s47E(d)	DPCSC	20 AUG 2008	2.2	Review and update
s47E(d)	DPCSC	NOV 2010	2.3	Review and update
s47E(d)	ADSCG	AUG 2014	3.0	Review and update to reflect new Privacy laws
s47E(d)	AD S&G, PSBS	NOV 2017	3.1	Review and update
s47E(d)	PSBS SPARA	DEC 2017	3.2	Review and update
s47E(d)	AD S&G, PSBS	DEC 2017	3.3	Review and update
s47E(d)	AD S&G, PSBS	SEP 2019	4.0	Minor updates, incremented for authorisation.
s47E(d)	PSBS SPARA	NOV 2019	4.1	Review and update
s47E(d)	PSBS SPARA	FEB 2020	4.2	Review and update
s47E(d)	PSBS SPARA	MAY 2020	4.2	Review and update
s47E(d)	PSBS SPARA	AUG 2020	4.3	Change password length from ten to 14 characters
s47E(d)	PSBS	SEP 2022	4.4	Update password character requirements, access to PI data obligations
s47E(d)	PSBS	DEC 2022	4.5	Review and update

AUTHORISATION

Document Authoriser	Version	Signature
Director People Systems Business Support	v4.5	

Proposals for amendment, or requests for copies of this Documentation Control Standard, are to be forwarded to:

Assistant Director S&G
s47E(d)
Department of Defence
CANBERRA ACT 2600

TABLE OF CONTENTS

DEFINITION OF TERMS

[redacted] – the Application has a system security rating of [redacted] where:

a. The highest classification of information processed on Personnel Management Key Solution (PMKeyS) is [redacted];

b. Access to an associated workstation is restricted to users with a minimum security clearance of Baseline as outlined in the Protective Security Policy Framework (PSPF); and

c. Access to PMKeyS is restricted to users who have a genuine 'need-to-know' requirement to view [redacted] data and have been granted formal approval.

Workstation – the term 'Workstation' refers not only to a computer unit (including Defence Protective Laptop) but to any storage and production media used in conjunction with a unit. This includes remote logon via DREAMS, the Home portal and media such as; removable drives for example USB Flash drives, separate printers and other storage devices.

PMKeyS – the term 'PMKeyS' includes the PMKeyS portal, Business Application, and Self Service. The term extends to Customer Relations Management (CRM) applications, including ComTrack Self Service (CSS), which are accessed via the PMKeyS Portal. Where aspects of this document relate to the PMKeyS Business Application only, the relevant paragraphs will include the words 'PMKeyS Business Application'. In all other cases this IS-SPP applies to the entire PMKeyS suite.

PMKeyS Data – the term 'PMKeyS Data' refers to data accessed directly through the PMKeyS application and/or sourced from PMKeyS reports, extracts and interfaces. The term also refers to data that is available through other applications that are automatically or manually loaded with data sourced from PMKeyS.

Human Resource Reporting Applications – this document does not specifically cover the access management arrangements for Human Resource Reporting Applications, including Management and Analysis Reporting Solution (MARS), Human Resource Metric System (HRMeS) and a data integration platform named InfoSphere; the Goals and Objectives of this IS-SPP apply to the Human Resource Reporting Applications. For details on access management practices and procedures for the Human Resource Reporting Applications, refer to the MARS Website.

PART ONE – GENERAL INFORMATION

Introduction

1. ICT Security in the context of PMKeyS concerns the control of data in PMKeyS. Security measures are implemented to ensure that data is stored, processed, transferred, and is adequately protected according to its sensitivity. The PMKeyS Security Operating Procedures, known as the PMKeyS Information System - Security Practices and Procedures (IS-SPP), are designed for a system security rating of ~~PROTECTED~~ and apply to the entire PMKeyS software suite.

2. PMKeyS is hosted on the Defence Protected Network (DPN) and is accessible directly via the DPN (including via Defence Protected laptops), through a DREAMS logon to the DPN, the Home portal, and through the deployable networks. PMKeyS is hosted on the Defence Protected Network (DPN) and is accessible directly via the DPN (including via Defence Protected laptops), through a DREAMS logon to the DPN, the Home portal, and through the deployable networks. This IS-SPP does not replace the Defence Security Principles Framework (DSPF), that outlines the responsibilities of all users' access to the DPN.Document Relationships

3. This IS-SPP is referenced to the Australian Government Information Security Manual (ISM), the Protective Security Policy Framework (PSPF), the Defence Security Principles Framework (DSPF), and the Australian Privacy Principles (APPs) as stated in the *Privacy Act 1988*.

4. Detailed instructions on the management of access to PMKeyS are provided on the PMKeyS – Access & Password webpage.

Audience

5. This IS-SPP is to be read prior to all users being granted access to the PMKeyS Business Application and/or the CRM and/or CSS Applications. It is a requirement that the IS-SPP is read and acknowledged by all users of PMKeyS.

Goals

6. The goals of this IS-SPP are to:

   a. Establish a standard set of security policy practices and procedures to be used by all users of PMKeyS;

   b. Reduce the risk of information loss by accidental or intentional disclosure, destruction or denial of access;

   c. Maintain the security, privacy, integrity and availability of PMKeyS and the data held in PMKeyS; and

   d. Ensure all personnel with access to PMKeyS take responsibility for the data they manage and/or use.

Objectives

7. To meet these goals, the following objectives must be achieved:

   a. Prevention of unauthorised access, disclosure, modification, manipulation, or deletion of PMKeyS data;

   b. Authentication of PMKeyS users;

   c. Establishment of security mechanisms that are flexible and responsive to changes in organisational structures and individual responsibilities;

d. Provision of means for identifying unauthorised access to PMKeyS and/or data and for taking appropriate corrective, preventative or disciplinary action;

e. Limit the use of PMKeyS to the purposes for which such resources are intended;

f. Ensure appropriate governance is in place for the security and privacy protection of PMKeyS data when accessed through applications and databases other than PMKeyS; and

g. Ensure that the system sponsor and/or delegates and authorised users are aware of their respective responsibilities with regards to maintaining the security of the data.

Scope

8. This is a 'living' document and its contents will be constantly monitored to ensure it is up-to-date and relevant.

9. The practices and procedures contained in this document are to apply to all data created, processed, and stored on PMKeyS.

PART TWO – PRACTICES AND PROCEDURES

General

10. PMKeyS has a security rating of [redacted] All users must be cleared to Baseline and have a 'Need-to-Know' requirement for data to which formal access has been approved. Depending upon the level of access requested, users requiring access to data for Protected Identities must have a minimum security clearance of Negative Vetting 1.

Conditions of Access

11. Before gaining access to the PMKeyS Business Application and/or the CRM application, personnel must:

a. Read and understand this IS-SPP.

b. Be aware of their responsibilities in using PMKeyS, as detailed in paragraphs 22 – 27 below.

c. Be granted as a minimum, a security clearance equal to the classification of Baseline. Higher security clearances are required for some levels of PMKeyS access.

d. Have a 'Need-to-Know' requirement to access the data for the purpose of performing assigned tasks.

e. Have been appropriately trained for the required PMKeyS access, and are competent to browse and/or transact in PMKeyS. Have completed the Campus courses mandatory for PMKeyS access; *Australian Privacy Principles eAssessment* and *Defence One Introduction & Reporting*. To gain access to the Global Payroll application, the *Defence One Introduction to Global Payroll* Campus course must also be completed.

f. Request PMKeyS Access via Self Service. This access request method is available to users where their Service or Group has mapped PMKeyS access roles to positions, and where the user has completed the prerequisite PMKeyS training courses. In cases where the PMKeyS roles to position have not been mapped, or access is requested for a CRM application, the user and supervisor are to complete Webform *AD688 Application for PMKeyS Access* form.

g. Access to Protected Identity data can only be granted with the agreement of the relevant Protected Identity authorisers.

12. **Supervisors** are to ensure that personnel using the Webform AD688:

a. Applied for the appropriate access required to perform their assigned tasks;

b. Met mandatory training requirements for the access requested; and

c. Read and understood this IS-SPP.

13. **Special Authorisation** is required before access can be granted to sensitive data including, but not limited to; Career Management, Discipline, Human Resource Budgeting, Drugs and Alcohol and Professional Development & Training. Additional detail is provided at paragraphs 32 – 33 below.

Password Management

14. Access to the PMKeyS portal is given to all ADF and APS personnel upon commencement. Access to the PMKeyS portal is only given to contractors where access to the PMKeyS Business Application has been authorised.

15. PMKeyS identifies individual users by their unique Operator ID and password. For APS and ADF users, the Operator ID is the user's Employee ID. For contractors, the Operator ID is the user's Other Defence Support (ODS) number (date of birth & initials), preceded by the letter C.

16. Users must change their password during their initial login. The password protects the user's account from unauthorised use. Passwords are classified as 'Official: Sensitive' and must not be revealed to any other person.

17. The following policies are to be enforced by PMKeyS on all user passwords:

a. Users are forced to change passwords every 90 days on the PMKeyS Portal for continued access to PMKeyS, Self Service and CRM;

b. Passwords must be a minimum of fourteen (14) characters in length and a maximum of thirty two (32) characters consisting of the following character sets:

(1) Lowercase alphabetic characters (a-z)

(2) Uppercase alphabetic characters (A-Z)

(3) Numeric characters (0-9)

(4) Special characters (! @ # $ % ^ & * ( ) - _ = + \ | { } [ ]; : ? / . ,)

c. The same password cannot be used in any 30-day password rotation; and

d. Users will be locked out after three consecutive failed logon attempts.

18. The PMKeyS Information Technology Security Officer (ITSO) is to be notified if a user's password is compromised, or suspected of being compromised. The PMKeyS ITSO is to log the details and initiate action for the compromised password to be changed.

19. Automated procedures for deletion of access to PMKeyS are documented on the PMKeyS website. Refer to the Access Purge Process on the Privacy & Security webpage.

20. The PMKeyS ITSO is responsible for monitoring and auditing the issuing of Operator IDs and passwords to authorised users. For a full description of the duties of the ITSO, refer to Annex A.

21. Users are required to set up their PMKeyS Portal password reset hint on initial login. Users who have forgotten their password (and have not set up a reset hint) or have a locked account are to contact the Defence Service Network (DSN) for assistance. Refer to the Password Management webpage.

User Responsibilities

22. All users must:

a. Abide by the policies, practices and procedures set out in this document; and

b. Report at once any attempted or actual breach of security to the PMKeyS ITSO via email s47E(d) ; and/or

c. Report any shared or suspected PI data spills by completing an XP188 form

23. It is the responsibility of all users to:

a. Maintain **confidentiality** and **integrity** of information stored on PMKeyS; and

b. Read and understand the PMKeyS IS-SPP prior to granting access to the PMKeyS , CRM and/or CSS Business Applications, or when notified that amendments have been made.

24. Supervisors are responsible for ensuring that a user has read, understood and complies with the PMKeyS IS-SPP.

25. No user is to attempt to bypass or defeat the security systems, or attempt to obtain use of passwords or privileges issued to another person.

26. All users must use their own account for specific work-related tasks only. Unauthorised changes to, or creation of, PMKeyS accounts is not permitted .Any suspected changes will be investigated as a breach.

27. Prior to granting access to PMKeyS, all users are to be made aware of their responsibilities and complete a declaration as acceptance of responsibilities. By signing an AD688 Application for PMKeyS Access form, or by accepting the *Privacy & Security Acknowledgement* when applying for PMKeyS access via Self Service, the user acknowledges they have read, understood, and accept the terms and conditions set out in this PMKeyS IS-SPP.

Privileged Users

28. The administration of PMKeyS permits certain users to hold accounts that enable a greater level of functionality than is offered by a standard user account. This includes maintenance personnel, security personnel, system administrators, database administrators and users granted privileged access as defined by the ISM. Those with privileged access have the same responsibilities under the IS-SPP as a standard user.

29. In accordance with ICT Security advice, privileged access accounts cannot be used via DREAMS or a Defence Protected Laptop. Privileged accounts can only be accessed on computers in secure Defence establishments using the Defence Protected Network.

30. Privileged user access are reviewed quarterly for compliance confirmation by the Security Policy Audit Requirements Analysis (SPARA) team in People Systems Business Support (PSBS) and/or their delegates. An access review can be conducted at any time by the user themselves, or the user's supervisor/manager.

31. Privileged users are required to maintain a correction log as documented in the Requirements webpage. The PMKeyS ITSO and/or their delegates/Business areas may conduct regular audits of correction logs to ensure compliance.

32. Special Authorisers are in place to ensure that personnel requesting access to PMKeyS have:

a. Requested the appropriate privileged access to adequately perform their assigned tasks;

b. Undertaken the required PMKeyS training and are competent to transact in PMKeyS;

c. Read and understood the PMKeyS IS-SPP; and

d. Understand the Australian Privacy Principles and how they apply to PMKeyS.

33. Special Authorisers are to ensure they are aware of their respective responsibilities and the responsibilities of the users they are authorising with regard to maintaining the security and privacy of information.

System Security Sponsor

34. The System Security Sponsor (Director PSBS) and/or their delegates are responsible for:

a. Conducting a review of the PMKeyS IS-SPP to ensure it continues to comply with the goals and objectives detailed in Part One (General Information) of this document;

b. Ensuring the implementation of, and sustained compliance by running monthly and quarterly reports, and engaging with customer to justify their requirement for accessing PMKeyS and meeting their obligations for security, the PMKeyS IS-SPP;

c. Resolving information system security issues in consultation with the PMKeyS ITSO;

d. Ensuring an ITSO is nominated for the PMKeyS application;

e. Ensuring that the ITSO and Security Manager carry out their duties in accordance with Annex A of this document; and

f. Ensuring that the current version of the IS-SPP is available for viewing by all users on PMKeyS via the Portal logon page, and on the PMKeyS website.

Access to PMKeyS Sourced Data through other Applications or Databases

35. PMKeyS data can be provided routinely or adhoc to other Defence and non-Defence applications and databases via interface or extract. To ensure appropriate security and privacy protection of the PMKeyS sourced data the following needs to occur before data will be provided:

a. any application or database that will store PMKeyS data must undertake analyse from CIOGs ICTSB team and be accredited as reliable and trustworthy.

b. the owners of the other applications and databases are to put in place Data Management Agreements (DMA) and procedures that adhere to Part One of this IS-SPP.

36. The Directorate of Workforce Information (DWI) is to ensure that a DMA is completed before PMKeyS data is provided to other Defence and non-Defence applications and databases. The DWI is to ensure that the DMA is distributed and endorsed by other data owners such as the Director of PSBS and the other system owner(s) as the recipients of the data.

37. For applications and databases outside Defence, DWI is to ensure that a DMA is completed before PMKeyS data is provided to these non-Defence applications and databases.

38. For Defence applications and databases being provided with PMKeyS data through a PMKeyS batch process, PSBS is responsible for ensuring appropriate security management is applied. This is required before PSBS signs off the System Change Request, Functional Specification, and User Acceptance Testing.

39. For Defence applications and databases being provided with PMKeyS data through a DWI provided extract, DWI is responsible for ensuring appropriate security management is applied.

Breaches of Security

40. All breaches of security are to be reported and investigated in accordance with the standards contained in ISM and DSPF. Any attempted or actual breach of PMKeyS security is to be reported to the PMKeyS ITSO via email s47E(d)).

41. Any user who has access to a Defence/Defence Industry domain or inter-domain connection will be in breach of security if they:

a. Attempt to access information and/or resources without the required authorisation, clearance, and/or briefing;

b. Attempt to access information and/or resources, and cannot justify their need for access;

c. Attempt to circumvent the access mechanisms that have been applied to protect information and/or resources;

d. Attempt to deny functionality of the system to any other person without prior authorisation;

e. Attempt to corrupt information that may be of value to Defence;

f. Do not take reasonable steps to confirm that the information that they originate will be protected;

g. Extract information from the system and pass it to a person who does not have an established ‘Need-to-Know’ requirement, or is not authorised to access that information;

h. Attempt to modify information and/or resources without authority; and

i. Process information that is classified above the level allowed.

42. The personal information contained within PMKeyS is subject to the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988*. The APPs provide legal direction on the collection, storage, use and disclosure of sensitive and personal data. Please refer to the Defence Privacy website for further information.

43. Intended, unauthorised, or inappropriate use or disclosure of personal information contained within PMKeyS is an infringement of the *Privacy Act 1988*. It is also a breach of the *Public Service Act 1999* Part 3, Section 13 (the APS Code of Conduct), and the *Defence Force Discipline Act 1982*. Such breaches may result in corrective action taken under the relevant provisions of the *Defence Force Discipline Act 1982*, or the *APS Code of Conduct Procedures*. Actions may include:

a. A reprimand;

b. Removal from part or all of the PMKeyS application;

c. Reduction in salary by way of a monetary fine;

d. Reduction in classification;

e. Termination of service with the Department of Defence; and

f. Civil charges.

ANNEX A

Duties of the PMKeyS Information Technology Security Officer (ITSO)

1. The PMKeyS Information Technology Security Officer is the PMKeyS Security Policy, Audit, and Requirements Analysis (SPARA) Team Leader within People Systems Business Support (PSBS). The PMKeyS ITSO is responsible to the System Security Sponsor and/or delegate for the following:

a. Perform administration in support of PMKeyS security and the application of Defence security policy and standards;

(1) Specifically analysing reports, queries or any extracts containing PMKeyS data including sensitive information, particularly for Users who have row security. (Access to view PI data)

b. Develop and implement PMKeyS security policy in consultation with PMKeyS stakeholders, and communicate with PMKeyS users;

(1) To exercise caution and be aware that reports will produce PI data unless configured to exclude PI units. (Please exclude PI Units' data when running reports, where there is no requirement for PI data output)

(2) That to share PI data is considered a breach or data spill, as this data cannot be viewed without appropriate PI authorisation

c. Ensuring procedures are in place to grant the appropriate PMKeyS access to personnel based upon the business authorised roles to be performed by the users requesting access

d. Perform and analyse quarterly audits of all listed 'Privileged Users'

e. Review and contribute to the relevant PMKeyS security training

f. Provide an escalation path to enable personnel to bring notice to all suspicious incidents, including;

(1) Investigations of all attempted or actual breaches of security; and

(2) Investigations of all attempted or actual data spills reported via XP188 forms

g. Prioritise the investigation of any attempted or actual data spills and implement risk management and policy changes to prevent these incidents re-occurring

h. Maintain a register of reported fraudulent and security breach incidents and forward to relevant identified authority as required; and

i. Act as the liaison between system personnel and assist in identifying and correcting security deficiencies.

Note: A Deputy PMKeyS ITSO, the SPARA APS 5, has been appointed and is able to perform all of the PMKeyS ITSO duties mentioned above in the absence of the Team Leader SPARA ITSO.

Duties of the PMKeyS Information Technology Security Manager (ITSM)

1. The PMKeyS Information Technology Security Manager is the PSBS Assistant Director of Security and Governance (AD S&G) and is responsible for the following aspects of the system management in relation to security:

a. Management of PMKeyS security policy.

b. Standards compliance is maintained in accordance with the ISM, DSPF and the *Privacy Act 1988*.

2. The PMKeyS Information Technology Security Manager is **not** to be the PMKeyS ITSO.