Establishment of the Office of the Special Investigator as an Executive Agency

Audit Report

Prepared for:

Office of the Special Investigator

December 2021

Synergy

Table of Contents

1. Executive Summary

1.1 BACKGROUND

As part of the Office of the Special Investigator's (OSI) Internal Audit Plan for 2021–22, an internal audit of the Establishment of the OSI as an Executive Agency was approved by the OSI Executive Board.

The OSI was established with the intent to address potential criminal matters raised in the Inspector-General of the Australian Defence Force's (ADF) Afghanistan Inquiry Report and to investigate with the Australian Federal Police (AFP) allegations of criminal offences under Australian law, arising from, or related to, any breaches of the Laws of the Armed Conflict, by members of the ADF in Afghanistan from 2005 to 2016.[1]

The OSI was established by an Executive Order signed by the Governor-General on 10 December 2020 and the Order commenced on 4 January 2021[2]. Prior to OSI's commencement, a Department of Home Affairs taskforce undertook the initial planning of OSI's establishment including key legislative, administrative and operational requirements needed to create and staff a new agency. The taskforce was disbanded in early February 2021 with ongoing implementation of the requirements undertaken by OSI employees.

The Department of Finance (DoF) launched the *Entity Start Up Guide* (the DOF Guide) in August 2020. The Guide outlines a broad range of actions that need to be undertaken in preparing and establishing a new Commonwealth entity. It contains relevant information on legislation, policies, frameworks and processes that apply to the commencement and operation of a Commonwealth entity. It focuses on the following matters:

- Accommodation
- Appointments and Staffing
- Communications and Media
- Funding and Financial
- Governance and Compliance
- Information Technology (IT) and Security
- Information Management
- Purchasing
- Risk and Insurance
- Shared Services
- Tax and Superannuation
- Work Health and Safety

1.2 AUDIT OBJECTIVE

The objective of this audit was to provide assurance that the OSI has been established in line with legislative obligations and best practice required for non-corporate Commonwealth agencies. This included assessing:

- Risk management arrangements and broader implications for the agency
- Progress against the establishment requirements of the agency
- Governance arrangements, including the operations of the taskforce
- Whether the principles outlined by the DoF Guide were followed (where applicable), including:
    - Records management

[1] Office of the Special Investigator (OSI), 2021, *Office of the Special Investigator*, viewed 16 August 2021 <https://www.osi.gov.au/home>

[2] Order to Establish the Office of the Special Investigator as an Executive Agency can be found at <https://www.legislation.gov.au/Details/C2020G01030>

- Financial management
- People management
- IT management

Appendix A details the method and approach taken for this audit. **Appendix B** provides a list of stakeholders interviewed as part of this audit.

1.3 CONCLUSION

Internal Audit found that the principles outlined within the DoF Guide were mostly followed and core legislation, administrative and operational tasks were implemented to ensure that the agency could effectively operate from establishment.

Internal Audit identified areas for improvement across the 'Governance and Compliance' element of the DoF Guide. Internal Audit raised two recommendations, both were rated as low risk and relate to the OSI developing a Complaints Handling Framework and undertaking a risk assessment when contacting with children to determine whether a Child Safe Framework is required to be developed.

Internal Audit noted there are a number of corporate artefacts still in development. Progress on the development of these artefacts is documented in the Governance Roadmap which is regularly updated and provided to the Executive Board and the Audit and Risk Management Committee (ARMC), including timeframes for completion. As per these timeframes, all artefacts are intended to be finalised by December 2021.

Since the OSI was established in January 2021, s 47E(d) [redacted] An important consideration is to ensure that the governance artefacts accurately reflect the OSI risk profile and operations, therefore their development has been paced to ensure legal and operational complexities can be addressed appropriately. The artefacts in development are listed in Section 2.1.

At the time of this Internal Audit, the Memorandum of Understanding (MoU) between the OSI and the Department of Home Affairs was close to finalisation. Interviews with stakeholders identified that the interim MoU arrangements provide sufficient clarity of roles and responsibilities regarding shared service arrangements provided by the Department of Home Affairs.

2. Key Findings

2.1 PROGRESS AGAINST THE ESTABLISHMENT REQUIREMENTS OF THE AGENCY

FINDINGS

Internal Audit found that:

- given the short timeframes, the process in establishing the OSI was efficient, effective and well-coordinated.
- a Governance Roadmap has been developed that outlines the timeframes and completion of remaining core governance documents within the agency. Internal Audit acknowledges that the development of these core governance documents have been paced with the intention to accurately reflect OSI's risk profile and operations, including its legislative environment. Internal Audit considers that progress reporting has been transparent.

DISCUSSION

During this internal audit, it was evident that the establishment of the OSI needed to occur promptly and within a short timeframe. Stakeholder interviews highlighted that the process in establishing the OSI was efficient, effective and well-coordinated.

The table below shows a brief timeline of establishment key dates.

Year	Date/Month	Key Event
2020	12 November	The Prime Minister announced the decision to establish the OSI.
	19 November	A Notice of Disposal Freeze was issued by the National Archives of Australia to ensure protection of records.
	Late November	OSI Taskforce was established and coordinated by the Department of Home Affairs.
	10 December	The Executive Council Order was approved to establish the OSI as an Executive Agency.
	16 December	The Minister for Home Affairs announced the appointments of the Director-General, the Special Investigator, and the Director of Investigations.
	22 December	OSI was listed as a non-corporate Commonwealth entity under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and the Director-General of OSI was named as the Accountable Authority.
	23 December	Expression of Interest (EOI) positions were advertised for a range of roles.
2021	4 January	• OSI was formally established as an independent agency within the Home Affairs Portfolio. • The Accountable Authority Instructions (AAIs) and Schedule of Delegations were signed by the Director-General. • OSI website went live. • A lease arrangement was in place with the Attorney-General's Department (AGD), s 47E(d). • IT Systems were in place. • Both the Director-General and the Director of Investigations commenced in their roles and were on-boarded. • Special Counsel was appointed

Year	Date/Month	Key Event
	1 February	The Special Investigator commenced in their role and was on-boarded.
	February	Governance Stocktake recorded, later called Governance Roadmap
	February	Key management positions filled including Chief Operating Officer, Chief Financial Officer and Deputy Director-General
	Mid-February	OSI Taskforce ceased operations.
	May	OSI received funding/appropriation within the budget.
	May	Special Counsel commenced review of IGADF materials
	May	Audit and Risk Management Committee established. First meeting held 10 May 2021.
	9 June to 3 July	1st Tranche of Investigators undertook training
	30 June	A MoU was signed between the OSI and the AFP on joint investigation arrangements.
	16 July	1st Tranche of Investigators sworn is as special members of the AFP
	11 August to 3 September	2nd Tranche of Investigators undertook their training
	28 August	OSI launched its own intranet

As outlined above, OSI developed a Governance Roadmap which informs the planning and development of key governance documents within the agency. This Governance Roadmap provides an overview of the status and timeframes of the various governance documents in development, supporting the OSI to meet its corporate and governance responsibilities. Governance documents that have been completed to date include:

- COVID safety Plan
- Risk Management Framework and Policy
- Strategic Risk Register
- Audit and Risk Management Committee Terms of Reference
- Audit and Risk Management Committee Charter
- Internal Audit Plan
- Internal Audit Charter
- Enterprise Risk Register
- Privacy Management Plan
- Privacy Policy –Website Content
- PID Policy –Website Content
- FOI Policy and Disclosure Log –Website Content
- External Communications Strategy
- Media SOPs
- Information Publication Scheme Agency Plan
- Accountable Authority Instructions
- Financial Delegations
- Rules for Spending Money
- Portfolio Budget Statements
- Portfolio Additional Estimates Statements
- 2021-22 Corporate Plan
- 2020-21 Annual Report

- Accounting Position Paper (policies, processes and assumptions for OSI financial reporting)
- Annual Financial Statements
- MoU Australian Federal Police
- MoU Attorney-General's Department (s 47E(d))
- MoU Home Affairs Portfolio Media Monitoring
- Direction by Director-General: Prohibition on seeking Afghanistan Inquiry information
- Staff Undertakings Register
- Communication arrangements between IGADF and OSI
- Threat Assessments: s 47E(d)
- Threat Assessments: s 47E(d)
- Operating under Home Affairs Agency Security Plan and Security Risk Management Framework.

Whilst many governance documents have been finalised and others well advanced, governance documents still in development include:

- Work Health and Safety (WHS) Policy
- Privacy Procedure
- Privacy Procedures (includes corrections requests, and privacy related complaints)
- Public Interest Disclosure Policy and Procedure
- Data Breach Response Plan
- Freedom of Information (FOI) Procedures
- Records Management Policy and Procedures
- Information and Data Governance Framework
- Agency Security Plan
- Conflict of Interest and Declarable Associations Policy and Register
- Fraud Control Plan
- Gifts and Benefits Policy
- MoU with the Department of Home Affairs, in relation to shared services arrangements
- Protocol with Department of Defence for Sharing Information

Discussions with stakeholders identified that the timeframes to develop these corporate governance documents will ensure these documents accurately reflect OSI's risk profile and operations. Further, the timeframes involved in the development of these core governance documents have been paced to ensure legal and operational complexities can be addressed appropriately, which has been an unfolding picture since the commencement of the OSI.

The Executive Board and the ARMC are regularly updated in terms of the progress on the development of these core governance documents. As per the timeframes in the Governance Roadmap, all artefacts are intended to be finalised by December 2021.

There are no recommendations in this section.

2.2 GOVERNANCE ARRANGEMENTS, INCLUDING THE OPERATIONS OF THE TASKFORCE

FINDINGS

Internal Audit found that:

- governance arrangements were implemented to support the timely establishment of the OSI, including the establishment of an OSI Taskforce and the development of MoUs
- the Taskforce managed and coordinated the project efficiently and effectively, through utilising subject matter experts, regular engagement/communications and clear lines of roles and responsibilities across all Taskforce members
- three MoU arrangements were developed with the AFP, the Department of Home Affairs and the Attorney General's Department. All MoUs provide sufficient clarity around respective roles and responsibilities. It was noted that the MoU with the Department of Home Affairs was close to finalisation during fieldwork for this Internal Audit

DISCUSSION

Governance arrangements were implemented to support the timely establishment of the OSI. These governance arrangements included establishing an OSI Taskforce as well as developing MoUs to support the effective operation of the OSI.

Taskforce

Internal Audit found that the governance and operational arrangements of the Taskforce were well managed and coordinated, due to leveraging the knowledge and expertise of subject matter experts, regular engagement and communications, and having clear lines of roles and responsibilities across all Taskforce members.

The Taskforce was established in late November 2020 to lead the establishment of the OSI. The Taskforce was coordinated by the Department of Home Affairs and included key members from all corporate enabling services and functions such as Governance, IT, Security, Finance, Human Resources (HR) and Communications. The implementation benefited from the expertise of DoF and Prime Minister and Cabinet (PMC) staff in relation to standing up a new agency. The Department of Home Affairs also regularly collaborated with other government agencies in relation to the nature of the work being performed by OSI, including the Department of Defence, AGD and AFP.

The Taskforce used a variety of mechanisms in order to manage and coordinate the project. This included developing a listing of key tasks that needed to be completed and were assigned to the relevant Taskforce member/s. This task listing enabled key activities to be prioritised, monitored and tracked. The Taskforce also held regular weekly meetings and ensured that the outcomes from each meeting, including key decisions and actions, were documented. All stakeholders interviewed agreed that this process worked well as a way of ensuring communication across functions and that tasks were progressing. Internal Audit found that the roles and responsibilities within the Taskforce were clearly designated.

MoUs

Due to the nature and operating environment of the OSI, three MoU arrangements were developed. One MoU was between OSI and AFP, relating to the investigative work that OSI is required to perform with the AFP. The other MoU arrangement was between OSI and the Department of Home Affairs, relating to providing corporate services to the OSI. The third MoU was with the Attorney-General's Department s 47E(d) .

MoU Arrangement between OSI and the AFP

On 30 June 2021, the MoU between OSI and AFP was finalised. This MoU outlines how the AFP will work with OSI to conduct joint investigations into the commission of criminal offences under the Australian law arising from or related to any breaches of the Laws of Armed Conflict by members of the ADF in Afghanistan from 2005 to 2016. Specifically, the AFP will provide operational functions in relation to conducting these Joint Investigations, including (but not limited to):

- Operational oversight of joint investigations
- Responsibility for the use of any statutory powers by AFP appointees who have been deployed to the joint investigation (AFP appointees)
- Selection, deployment and management of AFP appointees
- Responsibility for overseeing joint investigations conducted, including the presentation of these investigations to the strategic decision-making body of the AFP, the *Sensitive Investigations Oversight Board*
- Requiring AFP appointees, including OSI personnel who perform AFP special member powers, duties or functions, to adhere to all AFP governance, policies and procedures, where applicable to a joint investigation and/or investigative activity
- Issuing directions, procedures or similar to AFP appointees about information management or information quarantining arrangements
- Provision of AFP support services, including:
    - Access to AFP specialist functions s 47E(d)
    - Legal advice in relation to the exercise of AFP powers or any legislative authority or the conduct of investigations more generally

Internal Audit identified that this MoU arrangement provides sufficient clarity between the roles and responsibilities of the AFP and OSI in relation to undertaking investigative activities and other operational arrangements.

MoU Arrangement between OSI and the Department of Home Affairs

To support the timely establishment of the OSI, a shared services arrangement with the Department of Home Affairs was put in place to provide ongoing corporate services to the OSI, including IT, HR and finance functions. Under these shared services arrangements, OSI was able to leverage the Department of Home affairs' core governance policies and procedures and adapt these artefacts in accordance with OSI's risk profile and operations. The Taskforce ceased with the acknowledgement that some artefacts still required refinement and OSI agency input. Section 2.3.10 provides further information regarding these shared service arrangements.

The shared service arrangements provided by the Department of Home Affairs are outlined and supported by a draft MoU. During the fieldwork for this Internal Audit, this MoU was in the process of being finalised. This is a pilot arrangement for the Department of Home Affairs, which is seeking to be a shared services provider to other government agencies in the future. Through discussions with stakeholders, it was noted that the interim arrangements have been effective. Without a formalised MoU, a potential risk is that detailed service requirements are not defined, leading to a lack of clarity and/or either agency taking on additional tasks/requirements. Though, interviews with stakeholders did not identify that this risk had transpired. Further, it is noted that the OSI has adequately captured this risk within its strategic and enterprise risk registers, containing such detail as the cause of the risk, consequences, controls and developing controls.

Given the large number of the Department of Home Affairs contacts within the MoU, the OSI highlighted that it was beneficial that there is a designated point of contact in place serving as a coordination point between OSI staff and the Department of Home Affairs staff. If OSI had any queries relating to any of these corporate functions, these would then be sent through to this central coordination point.

There are no recommendations in this section.

2.3 ADHERENCE TO THE PRINCIPLES OUTLINED WITHIN THE DOF *ENTITY START UP* GUIDE

FINDINGS

Internal Audit found that:

- the principles outlined within the DoF *Entity Start Up Guide* (DoF Guide) were mostly followed and core legislation, administrative and operational requirements were implemented to ensure that the agency could effectively operate from establishment
- areas for improvement were identified within Governance and Compliance and IT and Security

DISCUSSION

In order to ensure that the agency could effectively operate from establishment, the following was prioritised by the OSI:

- ensuring that office premises were secured
- IT systems/access were set-up
- staff were identified and transferred over to the agency
- payroll and certain staff employment terms and conditions were arranged, including with seconding agencies and
- core governance documents such as financial delegations and AAIs were in place in order to be compliant with the PGPA Act

Internal Audit identified that principles outlined within the DoF Guide were mostly followed. The table below provides a summary of Internal Audit's assessment of the key actions/activities that have been implemented in accordance with the DoF Guide. It was identified that ten (10) out of twelve (12) key actions/activities were addressed and have been implemented. For the remaining two (2) key actions/activities, areas for improvement have been identified. For a detailed assessment against each of these actions/activities, refer to the sections listed within the following table.

DoF *Entity Start Up Guide* – Key Action/Activity	Internal Audit Assessment	Section Reference in Report
Accommodation	All principles have been addressed	Section 2.3.1
Appointments and Staffing	All principles have been addressed	Section 2.3.2
Communications and Media	All principles have been addressed	Section 2.3.3
Funding and Financial	All principles have been addressed	Section 2.3.4
Governance and Compliance	Most principles have been addressed and areas for improvement have been identified	Section 2.3.5
IT and Security	All principles have been addressed	Section 2.3.6
Information Management	All principles have been addressed	Section 2.3.7
Purchasing	All principles have been addressed	Section 2.3.8
Risk and Assurance	All principles have been addressed	Section 2.3.9
Shared Services	All principles have been addressed	Section 2.3.10

DoF *Entity Start Up Guide* – Key Action/Activity	Internal Audit Assessment	Section Reference in Report
Tax and Superannuation	All principles have been addressed	Section 2.3.11
Work Health and Safety	All principles have been addressed	Section 2.3.12
Key:		
All principles have been addressed		
Most principles have been addressed and areas for improvement have been identified		
None of the principles have been addressed		

2.3.1 Accommodation

Topics relating to accommodation within the DoF Guide include:

- Domestic Office Accommodation
- Arranging Accommodation
- Public Works Committee Reviews
- States and Territories

Domestic Office Accommodation

The DoF Guide refers to the Commonwealth Property Management Framework which supports the PGPA Act and supplements Division 1 of the Commonwealth Procurement Rules (CPRs). Provisions within this Framework are mandatory for all non-corporate Commonwealth entities and applies to any new non-corporate Commonwealth entities.

One of the requirements under the Commonwealth Property Management Framework is to adhere to the Property Services Coordinated Procurement Arrangements. These arrangements are a whole-of-government coordinated procurement arrangement that cover leasing and facilities management services for Commonwealth domestic office accommodation and shopfronts. These arrangements are managed by three Property Service Providers: Evolve FM Pty Ltd, Jones Lang LaSalle (JLL) (ACT) Pty Ltd and Ventia Pty Ltd.

Internal Audit identified that this requirement included within the DoF Guide was met. A Property Service Provider/Adviser, JLL, was assigned to OSI. JLL was responsible for finding available properties that met specific requirements and in accordance with the Commonwealth Property Management Framework and any State and Territory jurisdiction laws/requirements. Properties were sought across s 47E(d) . It is also noted that the Director-General was involved in arranging the s 47E(d) premises, with the arrangements s 47E(d) including consultation with the Special Investigator. The Department of Home Affairs manages the contracted relationship with JLL, on behalf of OSI, as part of their shared services arrangements.

Arranging Accommodation

The DoF Guide recommends that new entities consult with DoF in relation to specific property related requirements and lease arrangements as well as arranging for a Property Service Provider to be assigned to the entity. As outlined

above, JLL was assigned to OSI to assist in finding suitable properties as well as in managing their leases. Therefore, this requirement has been met.

Public Works Committee Reviews

The DoF Guide outlines that public works, including office fit-outs which meet relevant thresholds may be subject to oversight and evaluation by the Parliamentary Standing Committee on Public Works, as per the *Public Works Committee Act 1969*. This Act requires that all public works for the Commonwealth which are estimated to cost more than $15 million must be referred to the Committee. Upon reviewing the Parliamentary Standing Committee on Public Works Inquiries Register, it was evident that public works, including office fit-outs undertaken by OSI were below this threshold. As a result, public works were not required to be referred to the Committee.

States and Territories

The DoF Guide outlines that there may be State and Territory laws and requirements that may be applicable when arranging accommodation. Stakeholder interviews highlighted that JLL is responsible for ensuring that State and Territory laws and requirements are addressed/considered (see *Domestic Office Accommodation*).

There are no recommendations for this section.

2.3.2 Appointments and Staffing

According to the DoF Guide, topics covered within this section include:

- Appointments, and
- Staffing.

The DoF Guide also outlines that there are different legislative frameworks that entities need to consider in relation to appointments and staffing. These legislative frameworks include the *Public Service Act 1999*, *Defence Act 1903* and *Parliamentary Services Act 1999*. When establishing an Executive Agency like the OSI, staff must be engaged under the *Public Service Act 1999*.[3]

Appointments

The DoF Guide outlines that the appointment of the Accountable Authority will be governed by the enabling legislation or other relevant legislative requirements. The accountable authority of a Commonwealth entity has certain duties and responsibilities under the PGPA Act.

On 30 November 2020, both the Minister for Home Affairs and the Attorney-General signed a letter advising the Prime Minister that the Director-General would serve as the agency head of OSI (i.e. Accountable Authority) and have management and accountability responsibilities under the PGPA Act. This letter also outlined that a Special Investigator and Director of Investigations would be appointed, to support the Director-General.

The DoF Guide also outlines that remuneration and other terms and conditions for accountable authorities may need to be determined by the Remuneration Tribunal. Internal Audit evidenced that the salary and conditions of the Director-General were determined and set by the Remuneration Tribunal.

[3] Section 6(1) of the Public Service Act 1999

The DoF Guide also outlines that executive remuneration is publicly reportable. The specific remuneration amounts paid to the Director-General, Special Investigator and Director of Investigations (during the reporting period) were published within OSI's Annual Report. Remuneration ranges of other Senior Executive Staff were also published within OSI's Annual Report.

Staffing

- **Recruitment**

Section 22(2) of *Public Service Act 1999* states that the engagement of an Australian Public Service (APS) employee (including an engagement under section 72[4]) must be as:

- an ongoing employee; or
- for a specific term or for the duration of a specific task; or
- for duties that irregular or intermittent

Given that the OSI's lifecycle is unknown, it was initially determined that the majority of the staff would transfer to the OSI on secondments from Australian Government agencies such as AFP, the Department of Home Affairs and AGD.

There were two main groups of staff that were required to be temporarily transferred to OSI, including corporate and legal policy staff, and specialised investigators. The table below outlines the process for identifying and transferring staff within these two main groups:

Staffing Group	Process in Identifying and Transferring Staff
Corporate and Policy Support Staff	The majority of corporate and policy support staff were transferred from AGD. Further EOI positions were advertised on the Department of Home Affairs' HR system, OurPeople. These positions covered a range of positions from governance, administration, recordkeeping, security, finance, legal, HR and communications/media. The EOI was open for a twelve (12) month period from the date of advertisement. Applicants were considered against the vacancies available during this period.
Specialised Investigators / Analysts	To support the role and purpose of the OSI, highly experienced investigators and intelligence analysts needed to be identified and temporarily engaged to work on joint OSI/AFP investigations. These specialised investigators and analysts were identified through merit-based selection processes undertaken by the OSI, with support from various State police services. As part of their induction, these investigators and analysts were provided specialist training into the legislative frameworks relevant to war crimes and other legislative doctrine/powers.

[4] This is referring to Machinery of Government changes.

- **Terms and Conditions**

The DoF Guide outlines that employment terms and conditions, including pay rates, are established in each entity's industrial instruments.

As the majority of OSI staff are seconded into the agency, the employment terms and conditions of these staff are set by the Enterprise Agreement or Workplace Determination of their home agency. This includes leave entitlements, remuneration, tax/super contributions and other allowances.

There are no recommendations for this section.

2.3.3 Communications and Media

Topics relating to communications and media within the DoF Guide include:

- Website Domain Names
- Australian Government Branding Guidelines
- Whole of Government Advertising Arrangements
- Media Enquiries Policy
- Clear and Consistent Government Communication

Website Domain Names

According to the DoF Guide, Commonwealth entities are required to have a '.gov.au' domain name in order to ensure that the website can be identified as a government website. Internal Audit identified that OSI's website was established by the commencement date of 4 January 2021 and contains the correct domain name, as per the DoF Guide.

Australian Government Branding Guidelines

The DoF Guide outlines that a common, easily recognisable brand ensures clear and consistent branding across Australian Government departments and agencies. Guidelines have been developed to help entities ensure the Australian Government logo is consistently applied to products such as official Australian Government documents and publications. Internal Audit sighted evidence that the Australian Government logo was applied on the OSI website, in its Annual Report 2020–21 and other public facing documents.

Whole of Government Advertising Arrangements

The DoF Guide outlines that entities should ensure all advertising is placed through the Australian Government's Central Advertising System. This has not been applicable to the OSI to date.

Media Enquiries Policy

The DoF Guide outlines that new Commonwealth entities should consider developing a Media Enquiry Protocol to assist in responding to approaches from the media.

Internal Audit identified that OSI developed a Media Engagement Standard Operating Procedure which was presented to the Executive Board on 5 May 2021 and then finalised. This document outlines the process in triaging, assessing and responding to media enquiries, including the relevant approvals sought prior to submitting a response. This document also outlines that media enquiries are regularly documented and retained within a register.

OSI has also developed an External Communication Strategy, to assist in appropriately and clearly communicating the nature of OSI's work, building an understanding of its remit and objectives, and managing expectations. This Strategy includes communication goals, key messages, and who the key stakeholders and audiences are. It also explains the nexus with the AFP media and provides context on the identified strategic risk of adequately managing the expectations and perceptions of stakeholders, impacting negatively on the credibility of the OSI and its outcomes.

Clear and Consistent Government Communication

The DoF Guide outlines that the Australian Government Style Manual is the authoritative source of rules and guidance for government writing and editing. This Manual aims to make all government communications clear and consistent.

Internal Audit sighted evidence of media enquiry submissions being made to the OSI. The response to these enquiries were thoroughly consulted, to ensure that clear and consistent communications/messages were being applied across similar enquiries. Media Enquiry Templates were also developed to assist in providing clear and consistent communications.

There are no recommendations for this section.

2.3.4 Funding and Financial

Topics relating to funding and financial within the DoF Guide are:

- Funding Arrangements (Appropriations)
- Banking and Cash Management
- Budget and Mid-Year Update of Budget and Forward Estimates
- Portfolio Budget Statements
- Monthly Reporting (Actuals and Estimates)
- Annual Financial Reporting (Estimates and Financial Statements)
- Consolidated Financial Statements and Final Budget Outcome
- Providing Information to the Organisations and Appointments Register

The OSI Taskforce held meetings with DoF representatives who conveyed DoF requirements with regards to financial arrangements and reporting. Alongside the Taskforce, a finance working group was established which involved relevant agencies including DoF and the Department of Defence. A paper was developed by the working group entitled *Accounting Paper on the Establishment of the OSI*, outlining the Department of Home Affairs' responsibility for meeting OSI's financial reporting obligations as part of the provision of shared services. This provided the basis for the current MoU arrangements, which were being finalised during fieldwork for this Internal Audit.

Funding Arrangements (Appropriations)

The Government agreed initial funding for the establishment of the OSI in Mid-Year Economic and Fiscal Outlook (MYEFO) 2020-2021, with the final costs of establishment to be agreed between DoF, the Department of Home Affairs and the Department of Defence. The DoF Guide outlines that Commonwealth money cannot be spent without an appropriation. Further, the DoF Resource Management Guide 100 – *Guide to Appropriations* states that approval to spend relevant Commonwealth money can only be given where there is available unspent appropriation.

Alongside the Taskforce, the finance working group through the *Accounting Paper on the Establishment of the OSI* considered four different approaches with regard to interim funding arrangements, pending the availability of an appropriation (provided within the May 2021 Budget). It was agreed that interim costs on behalf of OSI would be managed by the Department of Home Affairs, AGD and the AFP, as these agencies had the capacity to absorb the additional costs in the short term by using existing unspent appropriations.

A separate cost centre within the Department of Home Affairs was established to specifically record OSI costs and expenses. Policy authority to allow OSI to report and reimburse expenses from the date of its establishment was provided through the 2020–21 Mid-Year Economic and Fiscal Outlook (MYEFO) measure and s 47C(1)

The OSI's appropriation was $41,592m in 2020–21 and $75,537m in 2021–22 established within the May 2021 Budget. Therefore, the requirement of the DoF Guide has been fulfilled with regards to establishing an appropriation.

Financial Reporting

The finance working group *Accounting Paper on the Establishment of the OSI* provided the basis of the Department of Home Affairs and OSI MoU outlining that the Department of Home Affairs is responsible for meeting OSI's financial reporting obligations as part of the provision of common administrative services, including:

- internal financial reporting and budgeting
- cash management and bank account establishment
- preparation of budget estimates and profiles
- preparation of monthly financial statements for reporting to Finance at the program level through Central Budget Management System (CBMS)
- preparation of annual financial statements and coordinate of the ANAO audit
- preparation of annual financial statements for reporting to DoF at the program level through CBMS
- preparation of the Supplementary Reporting Pack to DoF for whole of government financial reporting
- maintenance of appropriate financial and accounting records
- other financial reporting requirements as required

These financial reporting requirements are met using the same processes, workflows and record keeping requirements as the Department of Home Affairs, scaled where necessary for the size of OSI. Therefore, the requirements of the DoF Guide have been fulfilled with regards to establishment of financial functions.

Organisations and Appointments Register

The Australian Government Organisations Register (the Register) provides information on the function, composition, origins and other details of 1,305 Australian Government entities and bodies. The Register is based on information collected by portfolio departments.

New Commonwealth agencies are required to provide information to DoF for inclusion in the Register.

Internal Audit confirmed that this had occurred and OSI information has been included in the Register.

There are no recommendations for this section.

2.3.5 Governance and Compliance

The DoF Guide states that core requirements under the PGPA Act must be established, including:

- AAIs, Financial Delegations and Procurement
- Performance Reporting
- Audit Committee
- Fraud Prevention
- Public Interest Disclosure Scheme
- Complaints Handling
- Commonwealth Child Safe Framework

- Human Rights and Anti-Discrimination Obligations

AAIs, Financial Delegations and Procurement

The DoF Guide outlines that a new entity must issue AAIs establishing appropriate internal controls for officials in the entity, establish a delegations schedule and that the CPRs are followed.

The focus of the Taskforce was ensuring that the necessary arrangements were in place from the first day of establishment, including signed AAIs and Financial Delegations. This requirement was met as the AAIs and Financial Delegations were signed by the Director-General and came into effect on 4 January 2021. Internal Audit also evidenced that the AAI's were modelled on DoF's model AAIs.

Given OSI's shared services arrangements with the Department of Home Affairs, it was identified that OSI was able to leverage and adopt the Department of Home Affairs' Procurement Framework, which align with the CPRs. Therefore, the requirements of the DoF Guide have been met.

Performance Reporting

All Commonwealth entities must publish corporate planning and reporting documents under the PGPA Act, including Corporate Plans and Portfolio Budget Statements (PBS) and Annual Performance Statements and Annual Reports.

Internal Audit identified that the OSI had established their Corporate Plan 2021-22 which includes three (3) main activities, three (3) performance measures and six (6) performance metrics for each measurement. The OSI has published its Corporate Plan and its first Annual Report was tabled in Parliament in October 2021, which sets out achievements against the performance metrics and targets contained in the 2021-22 PBS and Corporate Plan. As a new Commonwealth entity, the OSI did not have a Corporate Plan for 2020–21 containing metrics that an established government entity would usually use to measure and report its performance against. Under the circumstances, the OSI's performance for the 2020–21 reporting period was measured against the performance metrics and targets contained in the 2021–22 PBS.

Audit Committees

The PGPA Rule requires accountable authorities of Commonwealth entities to establish an audit committee to review the appropriateness of their entity's financial and performance reporting, and systems of risk and internal controls systems.

Internal Audit identified that OSI had developed an ARMC Charter which outlines the role and function of the ARMC, including engagement with various members/stakeholders. This Charter was signed on 11 May 2021 by the Director-General. The ARMC held its first meeting in May 2021 and intends to meet four times a year. The ARMC comprises four independent members selected by the Director-General for having the skills, knowledge and experience relevant to the operations of the OSI. The ARMC's forward work plan was presented at the 29 September 2021 meeting.

Fraud Prevention

Commonwealth Fraud Prevention Guidelines ensures that any potential risks to the vulnerability of fraud are minimised.

Given time constraints in establishing the OSI, OSI relies heavily on the fraud control and integrity frameworks of the AFP and the Department of Home Affairs. At the time of fieldwork, OSI was developing its own Fraud Control Plan, as evidenced within their Governance Roadmap. It is noted that the ANAO audited the Department of Home Affairs' fraud control arrangements as part of the financial statements audit in 2020 and they were found to be effective.

Public Interest Disclosure Scheme

Commonwealth entities have obligations under the *Public Interest Disclosure Act 2013* in handling public interest disclosures concerning their agency and from their officials. This includes responsibility for investigating suspected wrongdoing, taking appropriate action in response, and managing any related reprisal risk to the discloser.

Internal Audit identified that public interest disclosure information is contained on OSI's website and outlines the process in making a disclosure. The website also outlines that an Authorised Officer will assess and handle the disclosure. It was noted that the Public Interest Disclosure Policy and Procedure are still in development, as evidenced within OSI's Governance Roadmap. These documents were due to be finalised by October 2021.

The Director-General appointed a number of authorised officers who can receive disclosures and has also delegated powers to investigate disclosable conduct within the meaning of the *Public Interest Disclosure Act 2013*.

Complaints Handling

The DoF Guide outlines that complaints handling is a predictable and necessary part of program and service delivery. Any complaints made and raised can feed into lessons learnt. Serious and unresolved complaints can be referred to the Commonwealth Ombudsman for further investigation.

The OSI has information on its website informing the public how OSI can be contacted. The OSI web-form provides a channel for members of the public to provide feedback. Through discussions it was identified that in relations to investigations, the AFP's or the Department of Home Affairs' Complaints Handling Framework could be referred to (if necessary).

However, the OSI should clarify the complaints handling policy and processes for its staff, including for investigative staff and corporate enabling staff, such as acknowledgement upon receipt of the complaint, escalation processes, timeframes to respond to the complaint, and how to reach desired outcomes in handling a complaint that minimise risk for the agency (see *Recommendation 1*).

Commonwealth Child Safe Framework

The Commonwealth Child Safe Framework is a whole-of-government policy that sets minimum standards for creating and embedding a child safe culture and practice in Commonwealth entities. This framework is mandatory for all Commonwealth non-corporate entities. Accountable Authorities of Commonwealth entities are responsible for the implementation of the Framework within their respective entity. One of the core requirements of this framework is to undertake a risk assessment annually in relation to activities of the entity, to identify the level of responsibility for, and contact with, children, evaluate risks to child safety, and put in place appropriate strategies to manage identified risks.

Currently, the OSI does not have its own Child Safe Framework. Through discussions it was identified that the AFP's Child Safe Framework applies to all staff working on the joint investigation who are AFP Members/Special Members (all investigators and analysts). This should be referred to and adhered to (if necessary).

However, as required by the DoF Guide, a formal risk assessment to determine what (if any) child safe policies and procedures might be required has not yet occurred for the OSI itself (see *Recommendation 2*).

Human Rights and Anti-Discrimination Obligations

The DoF Guide outlines that new entities need to be aware of their human rights and anti-discrimination obligations. It was identified that human rights and anti-discrimination obligations were considered and included within the staff induction packs, including information about appropriate workplace behaviours, discrimination and information on what to do if there is suspected inappropriate behaviour. The pack includes OSI's culture and values including acting with integrity, ethically, the types of behaviours that are unlawful and that inappropriate workplace behaviour may breach the APS Code of Conduct, Values and Employment Principles contained within the *Public Service Act 1999*, the *Work Health and Safety Act 2011* and anti-discrimination legislation. Further, Internal Audit sighted the draft MoU, which provided that the Department of Home Affairs will assist the OSI with management of official workplace behaviour and provide OSI staff with access to the APS Code of Conduct Foundational Framework through the intranet.

It is also highlighted that the OSI, in conjunction with the AFP, has designed a three-week course for investigators and intelligence analysts to support them to manage the unique challenges of OSI's work. The course included training on legislative frameworks relevant to war crimes, investigation doctrine and use of powers. As such, Internal Audit considers that this requirement has been met.

IMPACT

- In the absence of having a complaints handling policy and processes, complaints may not be handled in a consistent manner and can present greater reputational risks for the agency
- In the absence of undertaking a risk assessment regarding contact with children, OSI may not be complying with the core requirements listed within the Commonwealth Child Safe Framework, which is mandatory for non-corporate Commonwealth entities

RECOMMENDATIONS

Recommendation #1	OSI should develop a Complaints Handling Policy and Procedure.
Risk Rating	Low
Management Comments	Agreed. We note that the OSI has already developed a procedure for handling privacy requests, complaints and enquiries, relevant aspects of which can be adapted and broadened out to apply to complaints on more general matters.
Action Officer	s 22(1) , Director, Governance
Timeframe for Implementation	End 2021

Recommendation #2	OSI should undertake a yearly risk assessment regarding contact with children including identifying responsibilities for contacting children, evaluating risks to child safety, and put in place strategies to manage identified risks.
Risk Rating	Low

Management Comments	Agreed. OSI accepts this recommendation and will undertake an initial child safety risk assessment to determine next steps. Consultation with the AFP will be required for functions relating to joint OSI/AFP investigations, noting that investigators operate under AFP governance arrangements and the OSI will need to understand what arrangements the AFP has in place.
Action Officer	s 22(1), Director, Governance
Timeframe for Implementation	1st Quarter 2022

2.3.6 IT and Security

Topics relating to IT and security within the DoF Guide include:

- Protective Security Policy Framework (PSPF)
- Cyber Security Principles and Guidelines
- Digital Procurement and IT Investment
- Establishing and Maintaining Digital Assets

PSPF

The PSPF articulates protective security policy and provides guidance to entities to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security. Non-corporate Commonwealth entities that are subject to the PGPA Act must apply the PSPF.

Since establishment of the OSI, protective security advice, guidance and support was provided to OSI, under the shared services arrangements with the Department of Home Affairs. The Department of Home Affairs' Security Branch assisted OSI in providing advice and guidance in relation to setting up their security governance framework, and policies and procedures in line with the PSPF. This involved providing OSI with copies of the Department of Home Affairs' Agency Security Plan, Terms of Reference of their Security Committee and other core security governance policies and procedures around physical access and appropriate information handling practices. Under the MoU arrangement, the Department of Home Affairs' Security Branch will continue to provide protective security advice and guidance, whilst the implementation of the security framework and the monitoring of security practices falls within OSI's responsibility. As such, OSI has engaged a consultant to develop a security framework and provide related services to the OSI. This includes developing and finalising OSI's Agency Security Plan by November 2021.

The DoF Guide requires entities to appoint a Chief Security Officer (CSO) to have oversight and decision-making authority on all elements of protective security within the entity, as per the PSPF. At the 19 May 2021 Executive Board meeting, the Director-General appointed the Chief Operating Officer as the CSO for the OSI and the Director ICT as the Chief Information Security Officer. The OSI is in the process of recruiting an Agency Security Adviser to take the lead on maintaining and implementing the Agency Security Plan and related frameworks/documentation upon completion of the work by the contractor.

Cyber Security Principles and Guidelines

The Australian Government Information Security Manual (ISM) outlines a cyber security framework that entities can apply, using their risk management framework, to protect their information and systems from cyber threats. The ISM contains core cyber security principles and guidelines. One of these core cyber security principles includes appointing

a Chief Information Security Officer (CISO) to provide cyber security leadership. The appointment of the CISO is listed as a requirement under the DoF Guide.

A CISO was appointed in May 2021 by the Executive Board. As previously outlined, OSI is taking steps to implement the Agency Security Plan and related frameworks/documentation.

Digital Procurement and IT Investment

The Digital Transformation Agency (DTA) has developed guidance to assist entities in establishing their digital footprint, key tasks include IT procurement, data management and web-hosting. One of the requirements of the DoF Guide is leveraging the tools, mandatory and optional panels and frameworks produced by the DTA, for procuring technology goods and services for government.

Internal Audit identified that IT equipment needed to be procured in order to fit-out OSI's office premises. This included procuring laptops, desktops and IT network capability. The OSI, through its shared services arrangements with the Department of Home Affairs, adopted that Department's procurement policies and practices, which reflect the principles in the CPRs and use of the whole of government arrangements. As such, the Department of Home Affairs' Procurement Framework was leveraged in procuring relevant IT equipment.

The DoF Guide also requires entities to consult or receive advice from the DTA in relation to digital and IT investments. Internal Audit identified that OSI was able to leverage IT systems from their shared services and MoU arrangements with both the Department of Home Affairs and the AFP. In particular, the Department of Home Affairs would provide OSI with the use of TRIM for recordkeeping and corporate related purposes. The AFP would provide OSI with their case management system, *PROMIS*, in relation to OSI's investigative work. As such, OSI did not need to invest in any new technology.

There are no recommendations for this section.

2.3.7 Information Management

Topics relating to information management within the DoF Guide include:

- Copyright,
- Privacy,
- Freedom of Information Act, and
- Information, Records and Data Management.

Copyright

The DoF Guide outlines that non-corporate Commonwealth entities need to consider how the agency will manage Intellectual Property (IP) and the use of copyright material, in accordance with the Australian Government's IP Framework and *Copyright Act 1968*. The OSI website provides information about copyright pertaining to information on the website. Discussions with stakeholders also identified that OSI would be able to leverage the Department of Home Affairs' IP and copyright frameworks (if necessary) and there is legal expertise within OSI with a high awareness of any copyright issues. The OSI is also taking part in discussions regarding a single agreement for Commonwealth copying of copyright materials being led by the Department of Infrastructure, Transport, Regional Development and Communications.

Privacy

Commonwealth entities have obligations under the *Privacy Act 1988* (Cth) and the *Privacy Code 2018*. These obligations outline how an agency must handle personal information and the governance arrangements they must have in place to build a consistent and high standard of personal information management. These arrangements and privacy obligations are outlined on the following page:

- **Development of Privacy Policy**

According to the Governance Roadmap, it was identified that OSI's Privacy Policy/Procedure were still in development at the time of audit fieldwork and were due to be finalised by September 2021. Recent stakeholder interviews highlighted that the Privacy Policy has been finalised and Privacy Procedures are currently going through the final clearance process and is being finalised. The process for handling personal information, accessing and correcting personal information and submitting privacy complaints has been developed and is included on OSI's website.

- **Development of Privacy Management Plan**

Internal Audit identified that OSI has developed a Privacy Management Plan, which came into effect on 7 July 2021. The Privacy Management Plan outlines how a medium risk profile for privacy was reached, including factors taken account such as the amount of information OSI has, the sensitives of that information and the potential damage of information being shared inappropriately. This plan was approved by the OSI Executive Board, and it is under ongoing review, to ensure appropriate flexibility for its implementation.

- **Appointment of a Privacy Officer and Privacy Champion**

Internal Audit identified that both a Privacy Officer and Privacy Champion have been appointed through OSI's Executive Board. Stakeholders confirmed that these appointments have been made known to the Office of the Australian Information Commissioner (OAIC), as per the DoF Guide.

- **Development of Data Breach Response Plan**

The Governance Roadmap outlines that the Data Breach Response Plan is still in development and is due to be finalised by October 2021. The draft outlines that the response plan is intended to enable the OSI to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the Notifiable Data Breach scheme that commenced on 22 February 2018. This plan was undergoing clearance processes for finalisation during the fieldwork for this Internal Audit.

- **Development of Collection Notices**

When an agency collects personal information about an individual, it must take reasonable steps to notify the individual of certain matters, or to ensure the individual is aware of those matters. This is done through a collection notice.

Collection notices relating to corporate purposes are documented within a privacy statement on OSI's website. OSI's website states that "when we collect personal information, consistent with the requirements under the Privacy Act, we will notify you using a privacy collection notice, if it is reasonable to do so." Collection notices relating to law enforcement activities falls within the investigation/AFP remit.

- **Development of Privacy Impact Assessments**

Internal Audit identified that OSI has not yet conducted a Privacy Impact Assessment. The OSI's website notes that (in accordance with the *Australian Government Agencies Privacy Code 2017*) as Privacy Impact Assessments are completed for any high risk privacy projects, information about them will be published on the website. The OSI is also currently developing its Privacy Impact Assessment Procedures, as evidenced within the Governance Roadmap. These are due to be finalised in November 2021.

Freedom of Information (FOI)

Agencies are required to develop processes and procedures for managing FOI requests under the *Freedom of Information Act 1982* (FOI Act). FOI Act obligations are assessed and outlined below:

- **Mandatory Publishing Requirements**

The FOI Act requires agencies to publish specified categories of information under the Information Publication Scheme (IPS). This includes publishing information about an agency's organisational structure, functions and decision-making powers, statutory appointments, annual reports, arrangements for comment on policy proposals, information routinely released in response to FOI requests and provided to Parliament and operational information.

Internal Audit sighted that these specified categories of information (as above) are published on OSI's website. The website also contains links to where more detailed information can be found, within each of these categories.

Agencies must also publish a plan that explains how they will implement and administer their IPS. Internal Audit identified that OSI has prepared an IPS Agency Plan that outlines which information the agency proposes to publish for the purposes of the IPS, how, and to whom, the agency proposes to publish the information, and how the agency otherwise proposes to comply with the IPS. The IPS Agency Plan also outlines how the IPS will be implemented/administered. The IPS Agency Plan is accessible on OSI's website.

- **Request for Access to Documents**

Each person has a legally enforceable right under the FOI Act to obtain access to government documents, except if the documents are exempt or conditionally exempt from disclosure. Internal Audit identified that a summary of documents that may be exempt are outlined on OSI's website along with information outlining how requests for access to documents can be submitted.

- **Development of FOI Policy/Procedure to Ensure FOI Requests are Responded to Within Statutory Timeframes**

The DoF Guide outlines that agencies are required to develop processes and procedures to ensure FOI requests are responded to within statutory timeframes (i.e. 30 days unless otherwise extended under the FOI Act).

The Governance Roadmap lists that FOI Procedures are yet to be developed and are due to be finalised by the beginning of December 2021. However, OSI's website content regarding FOIs is in place, outlining the process in making and responding to FOI requests, including that a decision will made within 30 days unless otherwise extended.

The DoF Guide also outlines that staff and resources must be delegated under section 23 of the FOI Act to enable compliance with the FOI Act. The Director-General has delegated a number of officers to make and/or review decisions under the FOI Act – the authorisation was signed on 27 April 2021.

- **Internal Review**

According to the DoF Guide, agencies are required to develop processes to ensure applications for internal review of all FOI decisions occurs within statutory timeframes (i.e. 30 days). FOI information outlined on the OSI website meets this requirement. The website states that requests for an internal review should be submitted through the website, and OSI will advise of the outcome within 30 days.

- **Disclosure Log**

Documents released in response to an FOI request must be published on a disclosure log within 10 working days of release to the FOI applicant. Certain exemptions apply, including if the information is personal about any person, and if it would be unreasonable to publish the information. The OSI's website has functionality to record such information within the disclosure log. To date, the OSI has not released any documents in response to an FOI request and, as such, there are no documents within the disclosure log.

- **Report FOI Statistics**

Agencies are required to report FOI statistics to the OAIC at the end of each quarter. Stakeholders confirmed that FOI statistics are reported to the OAIC at the end of each quarter.

Information, Records and Data Management

According to the DoF Guide, new entities have responsibilities for ensuring that records and information are properly managed. An assessment against each of these responsibilities is outlined in the table below:

Responsibility	Assessment
Creating and Maintaining Records	There is a listing of key documents and records contained with the relevant TRIM reference.
Development of Records Management Policies and Procedures	According to the Governance Roadmap, Records Management Policies and Procedures are still being developed and finalised. These documents are due to be finalised by November 2021.
Establishment of Clear Lines of Responsibility for Records Management	As part of the Records Management Policies and Procedures being developed, lines of responsibility for records management will be included.
Informing National Archives to Develop Records Authorities	Internal Audit identified that there were active consultation and communications between the Department of Home Affairs and the National Archives of Australia in establishing and developing records authorities for OSI. In addition, the records authority for the OSI determined that there would be a disposal freeze, preventing records from being destroyed. This disposal freeze is a legal instrument, which was issued on 19 of November 2020.
Providing Adequate Resources for Records Management Activities	Following the establishment of OSI, a Records and Information Management Officer has been assigned.

- **Data Sharing**

The DoF Guide provides references to the *Best Practice Guide to Applying Data Sharing Principles*. This guide provides guidance to Australian Government agencies on when and how to safely and effectively share the data in line with five Data Sharing Principles. These principles are:

- Project – the purpose for sharing data
- Data – the level of detail in the data
- Settings – the environment in which the data will be used
- People – who is accessing the data
- Outputs – what results can be made public

During the establishment of OSI, it was identified that there is a substantial number of records held within the Department of Defence systems that would assist OSI within their investigative work. Many discussions were held between the Department of Home Affairs and the Department of Defence in relation to the transfer of records in a manner that would not compromise those records. The Department of Defence and the OSI have agreed a procedure where the OSI requests on behalf of the joint investigation information from the Department of Defence on an as need basis. This procedure enables criminal investigators to seek and obtain copies of relevant documents from the Department of Defence and to use those documents for investigative purposes.

Through discussions with stakeholders, a formalised process has been documented for requesting information from the Department of Defence.

- **Information Management**

The DoF Guide outlines that the National Archives of Australia sets standards for the management of Commonwealth information assets, through their *Building Trust in the Public Record Policy: Managing Information and Data for Government and Community*. It provides key information management requirements to enable agencies to appropriately manage information, records and data. The policy outlines three information management requirements, largely centred on effective governance and reporting structures, information management processes, practices and systems and identified areas of information management inefficiency and risk.

Internal Audit identified that OSI has appointed a Chief Information Governance Officer. According to the Governance Roadmap, an Information and Data Governance Framework is still in-development and is due for completion by November 2021. It is noted that an internal audit of information management relating to access controls and monitoring processes for managing OSI information across the various IT systems leveraged from shared service and MoU arrangements is included on the 2021–22 Internal Audit Program. This provides an opportunity to assess potential risks relating to information management at a time when OSI frameworks and policies would have had time to further mature.

There are no recommendations for this section.

2.3.8 Purchasing

Topics relating to purchasing within the DoF Guide include:

- Use of the Commonwealth Procurement Framework
- Use of the Whole of Australian Government procurement arrangements
- Use of the Whole of Australian Government travel arrangements
- AusTender
- BuyRight Tool
- Use of the Commonwealth Contracting Suite

The OSI, through its shared services arrangements with the Department of Home Affairs, adopted that Department's procurement policies and practices, which reflect the principles in the CPRs and use of the whole of government arrangements. Further, the Department of Home Affairs' Procurement Teams provided advice and support to OSI in undertaking procurement and contract management activities. As part of the draft MoU between OSI and the Department of Home Affairs, it is outlined that the Department will provide the OSI with a dedicated procurement specialist and provide general, specialist and user system support on all procurement matters including, but not limited to:

- Advice on basic interpretation of the CPRs, including Grant Framework requirements
- Advice on options for undertaking procurement processes, assistance in drafting documentation for Request for Quote or Request for Tender and associated documents, being part of evaluation panels, conducting reviews of outcomes, managing all AusTender requirements, and assistance with contract management
- Advice and services in relation to the procurement module
- Drafting paperwork for OSI approval and undertaking data entry relating to procurements
- Quality control of procurement data entry into system
- Development of training materials and training for individuals or teams

There are no recommendations for this section.

2.3.9 Risk and Insurance

Topics relating to risk and insurance within the DoF Guide include:

- Establishing a Risk Management Framework
- Insurance Services Provided by Comcover

Risk Management Framework

The DoF Guide outlines that accountable authorities are required to establish and maintain appropriate systems of risk oversight, management and internal controls for the entity.

OSI's strategic risk register was one of the first governance activities undertaken, in February and March 2021. It was developed with the assistance of Deloitte under a Department of Finance program for new entities. It is regularly reviewed by the Executive Board.

On 9 July 2021, OSI's Risk Management Framework was approved by the Chief Operating Officer. The Risk Management Framework outlines the process in identifying, analysing, evaluating, monitoring and reviewing risks within OSI, at both a strategic and operational level. Key accountabilities and responsibilities are also outlined within the Risk Management Framework. Risks are regularly considered and discussed at weekly Senior Management

Meetings, weekly All Staff Meetings and at the Executive Board meetings. Risks are also reviewed at each ARMC meeting.

OSI has developed a Strategic Risk Register. Interviewees highlighted the benefit in having a DoF representative on the Taskforce, as this representative was able to provide assistance and guidance in facilitating the development of strategic risks. These strategic risks are focused on five (5) areas, including reputational, operational alliances, enabling capabilities, people and resourcing and legal. Risks contained within the register were assessed in terms of its potential cause, consequence and likelihood. Risk ratings were applied and risk owners were assigned. Each risk also had an identified control/treatment.

Enterprise risks were in development from July 2021 and were presented to the Executive Board meeting in August 2021.

Workers compensation insurance, including insurance services provided by Comcover, are addressed within Section 2.3.12.

There are no recommendations for this section.

2.3.10 Shared Services

Topics relating to shared services within the DoF Guide include:

- Shared Services hubs
- DoF's core services
- Transition toolkit

Shared Services Hubs

The DoF Guide outlines that the Shared Services Program Providers Hubs focus on delivering common services to other agencies, driving efficiencies across the APS through increased scale and adopting best practice approaches.

Shared Services hubs are located in:

- Australian Taxation Office
- Department of Foreign Affairs and Trade
- Department of Home Affairs
- Department of Industry, Innovation and Science
- Services Australia
- Department of Finance – Service Delivery Office (SDO)

The Department of Home Affairs supports the OSI by providing certain corporate, IT and other services on a shared services basis. This supports OSI to meet its statutory responsibilities while maintaining a focus on core responsibilities. The shared service arrangements provided by the Department of Home Affairs are outlined and supported by a draft MoU. As previously stated, during fieldwork for this Internal Audit the MoU was close to finalisation. Discussions with stakeholders highlighted that the interim arrangements have been beneficial and provided sufficient clarity over roles and responsibilities. Further, stakeholders said that it was beneficial to leverage the Department of Home Affairs' established frameworks and utilise specialist knowledge, whilst OSI's own frameworks continue to be developed to be agency specific.

There are no recommendations for this section.

2.3.11 Tax and Superannuation

Topics relating to tax and superannuation within the DoF Guide include:

- Registering for an Australian Business Number (ABN)
- Registering for a Tax File Number (TFN)
- Registering for Fringe Benefits Tax (FBT)
- Registering for Goods and Services Tax (GST)
- Undertaking Business Activity Statements (BAS)
- Setting up superannuation arrangements for staff

Internal Audit sighted evidence that OSI had registered for its ABN and TFN. As the majority of staff were seconded from other agencies, the tax and superannuation details for these staff remained as per their Enterprise Agreements from their home agencies. Internal Audit sighted evidence of tax and superannuation arrangements set up for staff employed directly by the OSI.

As part of the draft MoU sighted by Internal Audit, the Department of Home Affairs manages BAS and GST requirements for OSI and submits BAS and GST on behalf of the OSI, through existing systems.

Further, the Department of Home Affairs manages FBT related data collection, calculations, compliance and monthly and annual accruals through established systems.

Thus, the requirements of the DoF Guide for tax and superannuation have been met.

There are no recommendations for this section.

2.3.12 Work, Health and Safety (WHS)

Topics relating to WHS within the DoF Guide include:

- Obligations under the *Work Health and Safety Act 2011*
- Establishing worker's compensation insurance (through Comcare)
- Obligations as a Rehabilitation Authority

In order to ensure the safety and health of staff, OSI engaged two Health and Safety representatives. The representatives play an important role in the partnership between senior management and employees by ensuring that workers have the opportunity to participate in decisions affecting their health and safety at work. In order to manage the ongoing risks relating to the COVID-19 pandemic, OSI developed a COVID Safety Plan to guide staff through the current pandemic. Additionally, OSI provided staff with a health and wellbeing induction pack when they joined the agency. This induction pack provided staff with resources and information relating to accessing health and wellbeing services.

Internal Audit noted that OSI's WHS Policy is still in development, as per the Governance Roadmap. This policy was due to be finalised by October 2021. As part of the draft MoU sighted by Internal Audit, the Department of Home Affairs provides specialist advice and relevant templates to assist the OSI in establishing safe workplace practices and early intervention processes.

Under the Draft MoU with the Department of Home Affairs, there is an array of support provided for OSI staff, including that the Department of Home Affairs will:

- establish and provide access for OSI staff, through the intranet, to pre-emptive support/early intervention programs. This includes exercise physiologists, psychological services, communicable disease experts, inoculations
- ensure OSI staff have access to the Employee Assistance Program and to Fit&Well, through the Department's intranet
- ensure there are mental health first aid officers and peer support officers available to OSI staff
- provide a clinician to establish OSI specific strategies and procedures
- consistently develop safe, appropriate health policies that will be applicable to and available for the OSI through the intranet
- provide leadership to the OSI in relation to the audit and assurance of contracted health services providers,
- provide a dedicated psychiatrist for OSI staff
- use existing procedures for monitoring, reviewing and identifying risks and opportunities for improving the delivery of health related services and outcomes for the OSI

An internal audit on WHS is scheduled to be conducted in 2021–22. That audit will review whether the OSI is compliant with its obligations under the WHS Act 2011 and has appropriate policies, procedures, activities and reporting in place. This provides an opportunity to assess potential risks relating to WHS at a time when OSI frameworks and policies would have had time to further mature.

Establishing Worker's Compensation Insurance (through Comcare)

The Comcare scheme provides a compressive package of benefits to assist an employee to recover from a workplace injury. Comcare requirements are also outlined in the draft MoU, including that the Department of Home Affairs ensured the OSI were provided the relevant Comcare forms for establishment and that the Department of Home Affairs will provide general and specialist advice regarding reconsiderations and tribunal matters. The OSI's responsibility is to complete initial Comcare documentation and submit to Comcare.

Comcover is the Australian Government's self-managed insurance fund and provides cover for all normally insurable risks to entities. To arrange Comcover services, agencies are required to complete a New Entity Information Questionnaire in order to set up the insurance account and access Comcover benefits. Evidence was sighted where a New Entity Information Questionnaire was completed and an insurance account has been established.

There are no recommendations for this section.

Appendix A: Method and Approach

s 47(1)(a), s 47(1)(b)

Appendix B: Stakeholders Consulted

The table below outlines the stakeholders consulted throughout this internal audit.

Name	Position	Date
Home Affairs Stakeholders		
Ben Wright	Acting Deputy Secretary, Chief Operating Officer Group Head of OSI Taskforce	18 October 2021
Megan Seccull	Assistant Secretary, Security Branch	12 October 2021
Elise Wattam	Assistant Secretary, Property	14 October 2021
Sarah Marshall	Assistant Secretary, Civil Commercial and Employment Law (OSI Taskforce)	14 October 2021
Abby Triparthi	Assistant Secretary, Technology Operations and Support Branch (ICT)	13 October 2021
s 22(1)	Acting Assistant Secretary - Director Financial Accounting and Assets	12 October 2021
s 22(1)	Director, Records Management	14 October 2021
s 22(1)	Assistant Director, Records Management	14 October 2021
s 22(1)	Director, Delivery Management Office (ICT)	13 October 2021
s 22(1)	Director, Partnership and Engagement (People and WHS)	13 October 2021
s 22(1)	Director, Staff Mental Health and Wellbeing	21 October 2021
s 22(1)	Assistant Director, Staff Mental Health and Wellbeing	21 October 2021
s 22(1)	Director, Executive Governance and Support	26 October 2021
s 22(1)	Acting Executive Officer, Chief Operating Officer Group (OSI Taskforce)	18 October 2021
OSI Stakeholders		
Catherine Fitch	Chief Operating Officer	27 October 2021
s 22(1)	Chief Financial Officer	27 October 2021
s 22(1)	Director, Communications	27 October 2021
s 22(1)	Director, Digital Experience (ICT)	28 October 2021
s 22(1)	Director, Governance	7 October 2021
s 22(1)	Assistant Director, Partnership and Engagement (People and WHS)	13 October 2021

Appendix C: Abbreviations

The table below outlines the abbreviations and acronyms used in this report.

Abbreviation	Title
AAIs	Accountable Authority Instructions
ABN	Australian Business Number
ADF	Australian Defence Force
AFP	Australian Federal Police
AGD	Attorney-General's Department
ANAO	Australian National Audit Office
APS	Australian Public Service
APSC	Australian Public Service Commission
ARMC	Audit and Risk Management Committee
BAS	Business Activity Statements
CBMS	Central Budget Management System
CDPP	Commonwealth Director of Public Prosecutions
CISO	Chief Information Security Officer
CPRs	Commonwealth Procurement Rules
CSO	Chief Security Officer
DoF	Department of Finance
DTA	Digital Transformation Agency
EOI	Expression of Interest
FBT	Fringe Benefit Tax
FOI	Freedom of Information
GST	Goods and Services Tax
HA	Department of Home Affairs
HR	Human Resources
IP	Intellectual Property
IPS	Information Publication Scheme
ISM	Information Security Manual
IT	Information and Technology
JLL	Jones Lang Lasalle (ACT) Pty Ltd
MoU	Memorandum of Understanding
MYEFO	Mid-Year Economic and Fiscal Outlook
OAIC	Office of the Australian Information Commissioner
OSI	Office of Special Investigator
PBS	Portfolio Budget Statements

Abbreviation	Title
PGPA Act	Public Governance, Performance and Accountability Act 2013
PM	Prime Minister
PMC	Department of the Prime Minister and Cabinet
PSPF	Protective Security Policy Framework
TFN	Tax File Number
WHS	Work Health and Safety

THE INVESTIGATION INTO ALLEGED WAR CRIMES IN AFGHANISTAN – SOME LEGAL ISSUES

The Hon Mark Weinberg AO QC
Special Investigator[1]
(with the assistance of s 22(1) , Legal Researcher to the Special Investigator)

Introduction

1. In March 2016, the then Chief of Army, General Angus Campbell, asked the Inspector-General of the Australian Defence Force, Mr James Gaynor, to inquire into rumours of serious misconduct by Australia's Special Forces in Afghanistan. It was said that some of the rumours potentially disclosed the commission of war crimes.

2. On 16 May 2016, Mr Gaynor appointed Major General Paul Brereton, a judge of the Supreme Court of New South Wales, to inquire into these matters.[2] The inquiry timeframe was eventually fixed as being between 2005 and 2016.

3. On 29 October 2020, Brereton J provided his report to Mr Gaynor.[3] The Report is detailed and extraordinarily comprehensive. Large portions of it remain redacted, particularly pt 2 which concerns the specific incidents, and issues of interest, with regard to which findings were made.

4. Justice Brereton concluded that there were some 39 designated incidents where rumours, allegations, or suspicions concerning a breach of the laws of armed conflict could not be substantiated. Of these, some 28 were the subject of detailed examination, and 11 were so obviously devoid of substance that they were simply discontinued.[4]

---

1 Speech delivered at the Legal Aid New South Wales Criminal Law Conference, 2–3 June 2021, International Convention Centre, Sydney.

2 The inquiry and resulting report will hereafter be referred to as the 'Brereton Inquiry' and the 'Brereton Report' respectively

3 The Hon PLG Brereton, AM, RFD, *Inspector-General of the Australian Defence Force Afghanistan Inquiry Report* (Redacted final report, 29 October 2020) ('Brereton Report').

4 Ibid 28 [14]

5. Justice Brereton found, however, that there was credible information with regard to 23 incidents in which one or more non-combatants, or persons *hors de combat*, were unlawfully killed by, or at the direction of, members of the Special Operations Task Group ('SOTG'), in circumstances which, if accepted by a jury, would constitute the war crime of murder (pursuant to s 268.70 of sch 1 of the *Criminal Code Act 1995* ('the *Criminal Code*')). He also found that there were two further incidents in which a non-combatant, or person *hors de combat*, was mistreated in circumstances which, if accepted by a jury, would constitute the war crime of cruel treatment (s 268.72 of the *Criminal Code*).

6. Some of these 23 incidents concerned a single victim, and some multiple victims. The incidents in question involved a total of 39 individuals who had been killed, allegedly murdered, and a further two who had been cruelly treated.[5]

7. A total of 25 current or former Australian Defence Force personnel were said to have been perpetrators, either as principals or accessories. Some of these 25 soldiers were alleged to have engaged in a single ac, constituting a war crime, while others were said to have committed multiple war crimes on several occasions.[6]

8. In the introduction and executive summary to his report, Brereton J observed:

> None of these are incidents of disputable decisions made under pressure in the heat of battle. The cases in which it has been found that there is credible information of a war crime are ones in which it was or should have been plain that the person killed was a non-combatant, or *hors-de-combat*. While a few of these are cases of Afghan local nationals encountered during an operation who were on no reasonable view participating in hostilities, the vast majority are cases where the persons were killed when hors de combat because they had been captured and were persons under control, and as such were protected under international law, breach of which was a crime.[7]

5 Ibid 29 [16](a).
6 Ibid 29 [16](b).
7 Ibid 29 [17].

9. Justice Brereton went on to observe that there was credible information concerning the use of 'throwdowns',[8] possibly designed to conceal deliberate unlawful killings, though not necessarily intended for that specific purpose.[9] He also noted that there was credible information that junior soldiers were required by their patrol commanders to shoot prisoners in order to achieve a 'first kill', a practice known as 'blooding'.[10] He recommended that the Chief of the Defence Force refer 36 specific matters to the Australian Federal Police (the 'AFP') for criminal investigation. Those 36 matters were said to have arisen out of 23 separate incidents and involve a total of 19 individuals.[11]

10. Self-evidently, and as a matter of law, the Brereton Inquiry could go no further than to assess whether there was credible information as to whether a person had committed a certain specified war crime (or disciplinary offence).[12] As Brereton J correctly observed, this could not constitute a finding of criminal guilt, nor even a finding to any standard that a crime of any kind had in fact been committed.[13] It could rise no higher than a finding that there were 'reasonable grounds for a supposition', warranting further investigation.[14] Clearly, it could not amount to a finding that there was admissible evidence to prove the matter before a court of law.

11. The Brereton Report makes it clear that almost all of the witnesses who gave evidence before the Inquiry did so only after having received a notice requiring them to answer questions.[15] Accordingly, they acted under statutory compulsion.[16] No witness had

---

8 The practice of placing foreign weapons or equipment on the bodies of 'enemies killed in action' so that photographs can be taken which depict the deceased as a legitimate target.
9 Brereton Report (n 3) 29 [18].
10 Ibid 29 [19].
11 Ibid 29 [21].
12 Ibid 27 [6].
13 See generally, *McGuiness v Attorney-General (Vic)* (1940) 63 CLR 73, 83–4 (Latham CJ), 100–2 (Dixon J); *Lockwood v The Queen* (1954) 90 CLR 177, 181 (Fullagar J); *Victoria v Australian Building Construction Employees' and Builders Labourers' Federation* (1982) 152 CLR 25, 147–58 (Brennan J).
14 Brereton Report (n 3) 30 [22], 153 [37].
15 Ibid 123 [22].
16 See generally, *Defence Act 1903* (Cth) s 124(2CA); *Inspector-General of the Australian Defence Force Regulation 2016* (Cth) reg 32.

his or her evidence tested by cross-examination by what might be termed an 'opposing party'.[17]

12. That said, Brereton J made it clear that his findings had not been lightly reached.[18] The Inquiry had sought eyewitness accounts, as well as corroboration. It had considered what it termed 'persuasive circumstantial evidence', and in some cases strong 'similar fact' evidence.[19]

13. Importantly, Brereton J concluded that he was not persuaded that those above the level of Patrol Commander (that is, broadly speaking, Corporal or Sergeant) could have responsibility for war crimes sheeted home to them. It was overwhelmingly at that level of seniority that responsibility resided.

14. Justice Brereton accepted that more senior officers, such as Troop, Squadron and Task Group Commanders, had to bear moral command responsibility for what had happened under their command. That did not, however, extend to legal responsibility for the crimes of their subordinates. He particularly excluded those involved at what he termed 'higher headquarters', on the basis that the senior personnel involved did not have a sufficient degree of command and control to attract the principle well-known in military law of 'command responsibility'.[20]

War crimes — a brief history

15. A war crime is a serious breach of international law committed against civilians or 'enemy combatants' during an international or domestic armed conflict.

16. For so long as man has been waging war, he has tried to find ways to legitimise, and delegitimise, different forms of conduct. More specifically, he has sought repeatedly to devise rules that govern the treatment of captives.

---

17 Brereton Report (n 3) 30 [23].
18 Ibid 30 [24].
19 Ibid.
20 Ibid 33 [35].

17. Of course, the main concern with the law of armed conflict was the actual conduct of wars involving states. The idea that criminal responsibility could attach to individuals engaged in military activity came about only in comparatively recent times.

18. It was not until the aftermath of World War II that there developed a strong impetus towards codification of the laws of armed conflict. The four Geneva Conventions of 1949, to which Australia is party, set out in detail such matters as the obligation to treat prisoners humanely, and to avoid the commission of certain broadly designated grave breaches, and serious violations of the laws of war.[21]

19. The *Geneva Conventions Act 1957* (Cth)[22] enables statutory effect to be given to the Geneva Conventions, but the actual substantive law governing war crimes is not to be found in those Conventions, but rather in the provisions of the *Criminal Code*, which make war crimes breaches of federal criminal law.

20. War crimes were first designated as such in the latter part of the 19th century. Long before that, however, rules of customary law had governed the way in which armed conflict should take place. It is interesting to note that such offences were recognised during the American Civil War. The Lieber Code, adopted in 1863, represents the first modern codification of war crimes.[23] The Hague Conventions of 1899 and 1907 took the matter a step further.[24] There then followed the Nuremberg Principles[25] and in

---

21 *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, opened for signature 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950); *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, opened for signature 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950); *Geneva Convention Relative to the Treatment of Prisoners of War*, opened for signature 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950); *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, opened for signature 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950) (collectively ' the Geneva Conventions ').

22 ('the *Geneva Conventions Act*').

23 Francis Lieber and Board of Officers, *Instructions for the Government of Armies of the United States, in the field* (D Van Nostrand, 1863) ('the Lieber Code').

24 *Convention with Respect to the Laws and Customs of War on Land*, signed 29 July 1899, 32 Stat 1803 (entered into force 4 September 1900); *Convention respecting the Laws and Customs of War on Land*, signed 18 October 1907, 36 Stat 2277 (entered into force 26 January 1910).

25 'Principles if International Law Recognized in the Charter of the Nuremberg Tribunal and in the Judgment of the Tribunal' (1950) II *Yearbook of the International Law Commission* 364, 374.

1949 the Geneva Conventions (which are located as Schedules to the *Geneva Conventions Act*). So far as both this country and the United Kingdom were concerned, war crimes were also recognised, and punished as such, during the Boer War.[26]

21. Neither the Nuremberg Charter,[27] nor the statutes of the International Criminal Tribunal for the former Yugoslavia[28] and the International Criminal Tribunal for Rwanda[29] specify the physical or fault elements required for the particular crimes with which they deal. That task was left to the Tribunals themselves, and they developed their own jurisprudence on this subject.

22. The Nuremberg Charter provided a modern and succinct codification of war crimes, namely:

> Violations of the laws or customs of war. Such violations shall include, but not be limited to, murder, ill-treatment or deportation to slave labour or for any other purpose of civilian population of or in occupied territory, murder or ill-treatment of prisoners of war … killing of hostages, plunder or public or private property, wanton destruction of cities, towns or villages, or devastation not justified by military necessity … [30]

---

26 The British 'Red Book', the Manual of Military Law, in use at the time of the Boer War covered such things as how to treat enemy combatants who had surrendered. In simple, but clear terms the rule was stated as follows:

> The first principle of war is that armed forces, so long as they resist, may be destroyed by all legitimate means. The right of killing an armed man exists only so long as he resists; as soon as he submits he is entitled to be treated as a prisoner of war.
>
> Peter Fitzsimons, *Breaker Morant,* (Hachette, 2020), 63.

It is a reproach to modern drafting that the definition of 'war crimes', as adopted by the Nuremberg Tribunal, required only some 73 words. The International Criminal Tribunal of the former Yugoslavia extended this to 239 words. The Rome Statute expanded the definition still further to encompass some 1,725 words, not including the elements of the particular offences constituting war crimes. The text of the Rome Statute was still largely based on the Hague Conventions of 1899 and 1907. The *Criminal Code* adopts a similarly prolix approach.

27 *Charter of the International Military Tribunal – Annex to the Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis*, 82 UNTS 280 (entered into force 8 August 1945) ('the Nuremberg Charter').

28 SC Res 827, UN Doc S/RES/827 (25 May 1993), as amended by SC Res 1877, UN Doc S/RES/1877 (7 July 2009).

29 SC Res 955, UN Doc S/RES/955 (8 November 1994) annex.

30 William Schabas, *The International Criminal Court: A Commentary on the Rome Statute* (Oxford University Press, 2nd ed, 2016) 221.

23. The drafting of the Rome Statute[31] was an extraordinarily complicated process. The parties were unable to reach agreement on many matters. This resulted in a number of compromises, and led to some of the difficulties associated with art 8, which is the key provision under the Rome Statute so far as war crimes are concerned.

24. The drafting of art 8 perpetuated an unfortunate distinction (which first emerged after World War II) between war crimes committed in 'international armed conflict', and those perpetrated in what is described as 'non-international armed conflict'. That distinction is, in turn, perpetuated in the provisions governing war crimes in the *Criminal Code*.

25. In addition, a distinction of dubious worth was drawn between 'grave breaches of the Geneva Conventions'[32] and what were termed 'serious violations of Art 3 common to the Geneva Conventions'.[33] For reasons that can only be explained in historic terms, the 'grave breaches' category is said to apply to 'international armed conflict', whereas the 'serious violations' category applies to 'non-international armed conflict'.

26. Put simply, an international armed conflict is an armed conflict between two or more States. A non-international armed conflict is an armed conflict within the territory of one of the parties to the Rome Statute.

27. In substance, an armed conflict of a non-international character must be one between the armed forces, and dissident armed forces, or other organised armed groups within the State. Those dissident forces, or other armed groups, must exercise control over a sufficient part of the territory of the State as would enable them to carry out sustained and concerted military operations.

---

31 *Rome Statute of the International Criminal Court*, opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002) ('the Rome Statute').

32 *Criminal Code* sub-div D.

33 Ibid sub-div F.

28. There is a vast body of writing, and a substantial body of international case law, dealing with the technical meaning of these two expressions.[34] The overwhelming consensus is that Australia's involvement in Afghanistan between about 2005 and 2013 concerned a non-international armed conflict.[35] Accordingly, the war crimes listed in sub-div F of s 268 of the *Criminal Code* are applicable to the investigation of war crimes by members of the Australian Defence Force in Afghanistan, but not those offences set out in sub-div D.

29. The Rome Statute did produce one critical achievement. It confirmed that individual criminal liability under international law extended to war crimes committed in non-international armed conflict, and was not confined to such crimes committed in armed conflict between States. Even so, some delegations resisted this significant extension of criminal responsibility, favouring instead the antiquated view that war crimes should be confined to international armed conflict.

The Criminal Code — the war crimes provisions

30. In 2002, as a direct response to the attacks upon the Twin Towers and the Pentagon, the federal government enacted legislation creating an entirely new series of criminal offences. In doing so, it incorporated the bulk of the provisions of the Rome Statute into the *Criminal Code* (which had, by then, been operative for five years). It must be said that the drafting of these new offences, including war crimes, left a good deal to be desired.

---

34 See generally, Deidre Willmott, 'Removing the Distinction Between International and Non-International Armed Conflict in the *Rome Statute of the International Criminal Court*' (2004) 5(1) *Melbourne Journal of International Law* 196; Emily Crawford, 'Blurring the Lines between International and Non-International Armed Conflicts — The Evolution of Customary International Law Applicable in Internal Armed Conflicts' (2008) 15 Australian International Law Journal 229; Marco Sassoli, 'International and non-international armed conflicts' in Marco Sassoli (ed), *International Humanitarian Law* (Edward Elgar Publishing, 2019) 204.

35 See generally, Brereton Report (n 3) 28 [12], 123 [21], 266–7 [8]–[12], 290 [14].

31. With regard to war crimes alone[36] (not counting genocide and crimes against humanity), the numerous variants of such offences were simply introduced into the *Criminal Code* without complete definition, but linked back to the general principles of criminal responsibility, which are contained in ch 2. Thus, the physical and fault elements which are outlined in that chapter, and which had been drafted several years earlier, suddenly found themselves awkwardly applying to an entirely new body of offences that were *sui generis*, and had never previously been part of federal criminal law.

32. Likewise, a number of the general principles set out in ch 2 involving, for example, defences to criminal charges were now suddenly applicable to areas of the law that had only recently been developed. Defences such as mistake, ignorance of the law, duress, self-defence, and lawful authority, all of which are recognised as general defences in the criminal law, now found themselves having to be accommodated to a new body of legal doctrine, arising entirely out of the conduct of armed conflict.

33. Chapter 2 also deals at length with what may be termed extensions of criminal responsibility. Thus, there are rules in that chapter governing attempt, complicity and common purpose, joint commission, commission by proxy, incitement, and conspiracy. These rules were clearly intended to be of general application and ought, therefore, be capable of being readily adapted to any criminal conduct. That should include offences which take place in the course of armed conflict. A moment's consideration will make it clear that there are special factors associated with the conduct of war which make it difficult to apply these broad ranging defences to particular acts which can take place in the heat of battle.

34. Special rules, largely taken from the Rome Statute (and some earlier instruments), were developed to deal with the criminal responsibility of commanders and other

---

[36] Of which there are 45 separate offences contained within sub-divs D and E of div 268, dealing with offences committed in the context of, and associated with, international armed conflict, and a further 33 separate offences contained within sub-divs F–H of div 268, dealing with offences committed in the context of, and associated with, armed conflict that is not an international armed conflict.

superiors for the acts of soldiers under their authority and control. In relation to war crimes (but not genocide or crimes against humanity), the *Criminal Code* provides for a defence of 'superior orders'. However, the scope of that defence is limited. It can only be invoked if (a) the person charged was under a legal obligation to obey the particular order, (b) did not know that it was unlawful, and (c) the order was not itself 'manifestly unlawful.'[37]

35. If one turns to some of the specific elements of war crimes under the *Criminal Code*, there is no shortage of difficulty. Even the apparently straightforward crime of murder under s 268.70 (as it stood until it was amended in December 2016) gives rise to problems. That offence, which in that form is the one applicable to the conduct of the Australian Defence Force ('ADF') in Afghanistan, appears as follows:

> **268.70 War crime—murder**
>
> (1) A person (the ***perpetrator***) commits an offence if:
>
> (a) the perpetrator causes the death of one or more persons; and
>
> (b) the person or persons are not taking an active part in the hostilities; and
>
> (c) the perpetrator knows of, or is reckless as to, the factual circumstances establishing that the person or persons are not taking an active part in the hostilities; and
>
> (d) the perpetrator's conduct takes place in the context of, and is associated with, an armed conflict that is not an international armed conflict.
>
> Penalty: Imprisonment for life.
>
> (2) To avoid doubt, a reference in subsection (1) to a person or persons who are not taking an active part in the hostilities includes a reference to:
>
> (a) a person or persons who are *hors de combat*; or
>
> (b) civilians, medical personnel or religious personnel who are not taking an active part in the hostilities.

36. It is clear that the physical element of murder under this section is the causing of death of another. The difficulty lies in how that physical element should be characterised.

---

[37] *Criminal Code* s 268.116.

37. Under s 4.1 of the *Criminal Code*, which deals with 'physical elements', it is provided that:

> **(1) A physical element of an offence may be**:
>
> (a) conduct; or
>
> (b) a result of conduct; or
>
> (c) a circumstance in which conduct, or a result of conduct, occurs.
>
> (2) In this Code:
>
> ***conduct*** means an act, an omission to perform an act or a state of affairs.
>
> ***engage in conduct*** means:
>
> (a) do an act; or
>
> (b) omit to perform an act.

38. In addition s 4.3 provides that an omission to act can constitute a physical element, but only if the law creating the offence makes it so expressly or impliedly. There must also be a duty to perform an act, which has been contravened by omission in circumstances where the duty in question is imposed by law.

39. Accordingly, the first task must be one of characterisation. Is murder, as a war crime under the *Criminal Code*, to be regarded as (a) a 'conduct' offence, (b) a 'result of conduct' offence, or perhaps even (c) a 'circumstance in which conduct, or a result of conduct' occurs? The fault element applicable to murder will depend upon the answer to that characterisation question.

40. It must be said that this characterisation issue has not been definitively resolved, and is one of particular difficulty. Various commentators have expressed competing views regarding the proper characterisation of an offence such as murder. There is textual support for all these views. Yet, the question is one of fundamental importance which must be addressed.

41. Turning to the issue of 'fault elements', div 5 of the *Criminal Code* (which is contained in ch 2) is, relevantly, in the following terms:

5.1 Fault elements

(1) A fault element for a particular physical element may be intention, knowledge, recklessness or negligence.

(2) Subsection (1) does not prevent a law that creates a particular offence from specifying other fault elements for a physical element of that offence.

5.2 Intention

(1) A person has intention with respect to conduct if he or she means to engage in that conduct.

(2) A person has intention with respect to a circumstance if he or she believes that it exists or will exist.

(3) A person has intention with respect to a result if he or she means to bring it about or is aware that it will occur in the ordinary course of events.

5.3 Knowledge

A person has knowledge of a circumstance or a result if he or she is aware that it exists or will exist in the ordinary course of events.

5.4 Recklessness

(1) A person is reckless with respect to a circumstance if:

(a) he or she is aware of a substantial risk that the circumstance exists or will exist; and

(b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

(2) A person is reckless with respect to a result if:

(a) he or she is aware of a substantial risk that the result will occur; and

(b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

(3) The question whether taking a risk is unjustifiable is one of fact.

(4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

…

5.6 Offences that do not specify fault elements

(1) If the law creating the offence does not specify a fault element for a physical element that consists only of conduct, intention is the fault element for that physical element.

(2) If the law creating the offence does not specify a fault element for a physical element that consists of a circumstance or a result, recklessness is the fault element for that physical element.

…

42. As can be seen, recklessness has a specific meaning under the *Criminal Code*. That meaning is very different from the notion of recklessness which applies to murder at common law. It also differs from instances where that term is used in State or Territory legislation.

43. Similar problems are likely to arise in relation to the various forms of extended liability under ch 2, at least insofar as they apply to the war crimes provisions in sub-divs D–H of ch 8. Although the *Criminal Code* uses the same language as at common law in relation to concepts such as complicity and common purpose, it is by no means certain that these provisions, upon their proper construction, will ultimately be held to bear that meaning.

44. Moreover, as indicated above, s 268.115 (which deals with the responsibility of commanders and other superiors as a form of extended liability) presents its own difficulties. Notions such as 'effective command and control', and 'effective authority and control' will have to be carefully considered. To what extent can this section be invoked to render even a platoon commander, perhaps at the rank of corporal or sergeant, liable for the actions of troops under his control?

45. There are also difficulties with the notions of 'knowledge' and 'recklessness', so far as they apply to sub-divs D–H. The failure by more senior officers, and/or troops, to take necessary and reasonable measures to prevent or repress the commission of war crimes, or to submit the matter to competent authorities for investigation and possible prosecution is also a fertile field for close analysis.

46. Because we are dealing with a code, and one which is in some respects incomplete, there are complex rules which determine how the task of construing terms well known to the common law should be carried out. These include terms such as murder.[38] These

[38] See for example, the approach taken to the offence of 'conspiracy' under the *Criminal Code* by the High Court in *R v LK* (2010) 241 CLR 177.

rules of construction are by no means easy to apply. This makes the task of evaluating whether there is, in fact, admissible evidence to support charges of war crimes under the *Criminal Code* a particularly difficult one.

47. In addition to the approach taken by the common law to the various offences now contained within sub-divs D–H, it may also be necessary, as part of the interpretative task, to have regard to the rules which have, for centuries, governed the conduct of armed conflict between States.[39]

48. As can be seen, those who drafted the Rome Statute were far more prescriptive than their predecessors. Article 9 of that Statute provides that the International Criminal Court ('ICC') is to be assisted by a document known as the 'Elements of Crimes', which helpfully sets out the physical and fault elements on a crime by crime basis. In enacting the *Criminal Code*, Parliament seems to have relied heavily upon that document as the basis for specifying relevant definitions of the offences in sub-divs D–H.

49. The entire structure of the *Criminal Code* and, in particular, its treatment of the general principles of criminal responsibility, has created difficulty for judges in the past. The Code makes clear that for an offence in which the only physical element is conduct, the fault element is intention (as defined). Despite this, the Code lends no assistance when considering how a particular offence should be characterised, whether as one of conduct, circumstances, or result.

50. It should be noted that s 268.115 of the *Criminal Code*, in dealing with command responsibility, largely replicates art 28 of the Rome Statute. There is, however, one significant difference. The *Criminal Code* substitutes a recklessness standard for the Rome Statute's lower threshold of 'should have known'. This makes it more difficult

---

[39] See, for example, the case of Peter von Hagenbach, who was tried in 1474 by an ad hoc tribunal set up by the Holy Roman Empire. Some commentators regard this as the first international war crimes trial, with the added feature that the trial itself dealt with the theory of command responsibility. His defence was one of superior orders. It failed, and he was beheaded. See, further, the Battle of Crecy, in 1346, which was renowned in part due to the edict of the French King Phillip VI that no prisoners were to be taken.

to establish the fault element, in prosecuting a soldier under the command responsibility provisions of the *Criminal Code* than would be the case under the Rome Statute.

The special problem of use and derivative use immunities

51. As indicated, the vast majority of persons who gave evidence before the Brereton Inquiry gave evidence under compulsion. In his final report, and in relation to the powers he had exercised, Brereton J commented:

> Every witness who gave evidence to the Inquiry has the protections and immunities afforded by the *Defence Act*, s 124(2CA), and the Inspector-General of the Australian Defence Force Regulation, s 31 (prohibition against taking reprisals), s 32 (self-incrimination) and s 33 (protection from liability in civil proceedings). Those protections and immunities include *use* and *derivative use* immunity: under *Defence Act* s 124(2CA) and the Inspector-General of the Australian Defence Force Regulation s 32(2), any information given or document or thing produced by the witness, and giving the information or producing the document or thing, and any information document or thing obtained as a direct or indirect consequence of giving the information or producing the document or thing, are not admissible in evidence against the individual in any civil or criminal proceedings in any federal court or court of a State or Territory, or proceedings before a Service Tribunal, other than proceedings by way of a prosecution for giving false testimony.
>
> The immunities operate in any relevant court or Service Tribunal in which proceedings may be brought, and regulate the admissibility of certain evidence in those proceedings. They do not directly constrain the Inquiry, the Inspector-General of the Australian Defence Force, or for that matter the Chief of the Defence Force, in the use or publication of the Inquiry's findings or evidence before it. However, there is potential for criminal proceedings to be compromised if immunised evidence informs a prosecution. That is one reason why it is inappropriate for the evidence that has been obtained by the Inquiry to be published at this stage.
>
> It is important to observe that the immunities preclude only the admission in evidence in court proceedings of information given to the Inquiry by a witness (and anything obtained as a direct or indirect consequence) *against that witness*. They do not preclude the admission in evidence in court proceedings of information given to the Inquiry by a witness (and anything obtained as a direct or indirect consequence) *against any other person* – including another person who was also an Inquiry witness.[40]

52. In his Executive Summary, Brereton J further observed:

> Because of the immunities, explained above, to which witnesses who give evidence to the Inquiry are entitled, which preclude the use of a person's evidence to the Inquiry,

---

40 Brereton Report (n 3) 38–9, [63]–[65].

> or anything discovered as a result, in proceedings *against that person*, there are some individuals who have been involved in misconduct who will not be amenable to prosecution. That is the necessary consequence of their having made protected disclosures to the Inquiry, without which the conduct described in this Report would not have been uncovered. Decisions therefore have to be made about which individuals should, and which should not or cannot be prosecuted. Ultimately, those are decisions for prosecuting authorities. However, the Inquiry's recommendations have taken this issue into account. Essentially, this involves prioritising a hierarchy of criminal responsibility, in order that those who bear greatest responsibility should be referred for criminal investigation, and potentially prosecution, in priority to those bearing less responsibility.
>
> The Inquiry's approach is that those who have incited, directed, or procured their subordinates to commit war crimes should be referred for criminal investigation, in priority to their subordinates who may have 'pulled the trigger.' This is because in a uniformed, disciplined, armed force those in positions of authority bear special responsibilities, given their rank or command function, because their subordinates would not have become involved but for their instigation of it; and because what happened was entirely under their control, with their subordinates doing what they were directed to do.
>
> Additional factors include the objective gravity of the incident (for example, if there are multiple victims); whether the conduct appears to have been premeditated, wanton or gratuitous; and whether the individual concerned is implicated in multiple incidents, particularly if those other incidents may provide tendency evidence.
>
> The Inquiry has not recommended referral for criminal investigation where it appears that the use and derivative use immunities to be found in the *Defence Act 1903* and the *Inspector-General of the Australian Defence Force Regulation 2016* would deprive a prosecution of critical admissible evidence.
>
> The Inquiry recommends that any criminal investigation and prosecution of a war crime should be undertaken by the Australian Federal Police and the Commonwealth Director of Public Prosecutions, with a view to prosecution in the civilian criminal courts, in trial by jury, rather than as a Service offence in a Service Tribunal.[41]

53. The conferral of a derivative use immunity upon those who were compelled by notice to give evidence before the Brereton Inquiry clearly requires great care to be taken on the part of investigators and prosecutors to ensure that they do not make impermissible use of such testimony. Not only is the evidence so obtained inadmissible in any criminal trial, but there may also be other risks associated with any use at all having been made by investigators or prosecutors of compelled, and therefore protected, evidence.

---

41 Ibid 40, [70]–[74].

54. As will be seen, the OSI is well attuned to these risks. It is undertaking its work with great care in order to ensure that the suite of protections afforded to those witnesses who were compelled to give evidence before the Brereton Inquiry is given its full and lawful weight.

The creation of the OSI

55. Justice Brereton, having found that there were a number of cases of possible war crimes which warranted investigation (some of them involving allegations of the most egregious nature), was faced with the question of what then should be done. From his perspective, and self-evidently, it would have been unthinkable for the government to have ignored his findings.

56. As indicated, Australia is a party to the Rome Statute. The principle of complementarity, which underlies the creation of the ICC, dictates that if a country is unwilling, or unable, to carry out a proper investigation into alleged war crimes, and to prosecute those who have committed such acts, the ICC may assume jurisdiction over such matters.

57. If the Government were to fail to act upon the Brereton Inquiry findings, ADF members could find themselves the subject of criminal proceedings before the ICC. There is little doubt that most Australians would prefer to have these matters dealt with in accordance with our own system of criminal justice. They, of course, trust their own courts to deliver justice in a fair and impartial manner.

58. Justice Brereton had little to say about how, in his view, the matters which he raised should be investigated. It is well known, and has been widely reported, that as far back as 2019, the AFP became involved in an investigation into several possible war crimes in Afghanistan. In fact, the media has reported that the AFP had submitted two briefs of evidence to the Commonwealth Director of Public Prosecutions ('DPP') for her consideration.

59. Of course, the other cases considered by the Brereton Inquiry could also have been referred to the AFP for investigation. Why, then, did the Government ultimately conclude that it was preferable to have a new entity, the Office of the Special Investigator ('OSI'), take charge of that task?

60. There are probably several answers to that question.

- First, Brereton J acknowledged that despite the length of time that he had devoted to the task of preparing his report, he had not been able to complete his investigation into all of the allegations of war crimes that had been raised with him.
- Secondly, it is fair to say that the Brereton Inquiry had been confronted with a monumental task, even though it was concerned with determining only whether there appeared to be 'credible information' supporting the rumours that had been circulating for some years. The task of determining whether there is sufficient credible and admissible evidence to warrant the laying of charges is very different, and far more daunting.
- Thirdly, had the AFP been asked to investigate all of the matters that Brereton J had considered (as well as those that he had been unable to fully investigate), it would have had to allocate significant, and no doubt scarce, resources to that task. In addition, it could reasonably be anticipated that there would be many additional allegations of war crimes that had not been the subject of the Brereton Inquiry's attention. This has proved to be the case.
- Fourthly, it must be acknowledged that the work traditionally undertaken by the AFP is somewhat removed from the standard investigation of homicide, which is traditionally a matter for State and Territory police.
- Finally, there is a great deal of difference between the investigation and prosecution of offences under ordinary domestic law, and the consideration of international criminal offences of the type set out within div 268 of the *Criminal Code*. Put simply, investigators who are to examine allegations of this kind must be thoroughly versed in at least some of the intricacies of

international criminal law. They must also have a good working understanding of the different rules of evidence, and criminal procedure, which apply in the various States and Territories. In other words, this work is highly specialised, and requires a good deal of training. It should be done by a carefully selected group of police officers, all of them dedicated to this difficult task.

61. It was against this background that the Government determined in November 2020 that an entirely new body should be established. It should review the findings of the Brereton Report, and also consider other allegations of war crimes that had been levelled against ADF members in relation to their service in Afghanistan. This new body would be required to consider whether there was sufficient evidence that was both credible, and admissible, to warrant laying charges against particular individuals. If so, it would prepare briefs of evidence for submission to the Commonwealth DPP. As a result, the OSI was established.

62. In addressing the Senate Estimates Committee for Legal and Constitutional Affairs ('the Senate Estimates Committee') on 22 March 2021, the Director-General of the OSI, Mr Chris Moraitis, made it clear that the OSI would work closely with the AFP to investigate the potential criminal matters raised in the Brereton Report. In addition, it would investigate any new allegations of criminal offences under Australian law by members of the ADF in Afghanistan. He added that where appropriate, the OSI would develop and refer briefs of evidence to the Commonwealth DPP for consideration.

63. Mr Moraitis reported that since the OSI had commenced work on 4 January 2021, it had been focussed on establishing the appropriate workforce, structures, systems, and protocols which would underpin its independence from government. He stressed that the OSI would conduct an impartial and rigorous process.

64. Mr Moraitis further reported that, to date, the OSI had made good progress in engaging experienced investigators, as well as legal, governance and other support

staff. He noted that recruitment was then underway for joint teams of suitably qualified investigators and analysts from the AFP and State and Territory police services. That recruitment process was continuing and ongoing. A number of experienced police officers, all of whom were of the highest quality and integrity, had joined the investigative team of the OSI. As at the date of this paper, those officers are in the process of undergoing rigorous education and training.

65. Mr Moraitis recognised that the task that confronted the OSI would be challenging. In that regard, he pointed out that the Brereton Inquiry had made extensive use of statutory powers to compel SOTG members to provide information, without the protection of the privilege against self-incrimination. That, of itself, gave rise to the derivative use issue that I have previously mentioned.

66. Mr Moraitis indicated that, in order to ensure the integrity of any future prosecutions, the OSI had engaged an experienced and senior team of lawyers from the Australian Government Solicitor, to act as a 'Special Counsel Team'. He noted that their role had been, and still is, to advise the OSI of the legal principles that would guide its access to the Brereton Report, and to the information that had been provided under compulsion to the Inquiry.

67. As the Prime Minister made clear, the OSI would continue in existence for so long as was needed to fulfil its functions and discharge its responsibilities. At the same time, the OSI understands that its work must be undertaken expeditiously, though always bearing in mind the need for appropriate caution. Decisions regarding the bringing of criminal charges in an area such as this will never be taken lightly.

68. Mr Moraitis told the Estimates Committee that the OSI had already established effective working relationships with the AFP, the Department of Defence, and the Commonwealth DPP, as well as the Department of Foreign Affairs and Trade, and the Attorney-General's Department. However, as he made clear, none of those bodies would, as such, be involved in any investigations, or governance matters, that might impact the independence of the OSI.

69. For completeness, Mr Moraitis appeared again before the Senate Estimates Committee on 25 May 2021. On that occasion, he said:

> As previously advised, Ross Barnett is our Director of Investigations. He is supported by two Commanders to lead the investigations, and the initial cohort of 24 investigators and analysts (the first of up to 75) has now been selected and will join us shortly.
>
> These specialist investigators are being drawn from state police services and the Australian Federal Police, consistent with this work being a national effort. All investigators, no matter their home jurisdiction, will be sworn in as Special Members of the AFP. They will be based in a Sydney workspace.
>
> In close cooperation with the AFP, a substantial induction training program is being delivered soon to prepare these investigators and analysts for the challenging task ahead – investigating potential criminal matters raised in the Brereton Report and any new allegations of criminal offences under Australian law by members of the ADF in Afghanistan from 2005 to 2016.
>
> We have started receiving information relevant to our mandate and are focussed on ensuring this sensitive information is handled appropriately, to protect the integrity of our joint OSI-AFP investigation and any future potential prosecutions.
>
> Most of that information will come to us via our Special Counsel, which as I outlined in March, is now undertaking the important function of a quarantined review of the Inquiry information – as well as some new material – to ensure investigators only receive information they can lawfully use.
>
> We look forward to having the first tranche of investigators on board – ably supported by our corporate and legal team – and progressing the investigations as expeditiously as possible.
>
> As I advised the Committee in March, I will remain focussed on ensuring the appropriate workforce, structures, systems and protocols are in place to underpin our independence and our ability to conduct an impartial and rigorous process.[42]

70. As can be seen, a considerable amount has been achieved within a very short period of time, given the magnitude of the task that confronts the OSI. The work is challenging, at both a legal and factual level.

---

42 Opening statement to the Senate Estimates Committee for Legal and Constitutional Affairs, Parliament of Australia, Canberra, 25 May 2021 (Chris Moraitis, Director-General).

Conclusion

71. This paper presents only a small snapshot of some of the many legal issues that confront the OSI. The work that lies before it is unlike any that I have previously encountered. It is work that must be approached with care and sensitivity, but also with rigour, thoroughness, and dispassion. That is exactly what OSI will strive to achieve.

\- - - - -