RAND AUSTRALIA

Designing a Capability Development Framework for Home Affairs

Peter Dortmans, Jennifer D. P. Moroney, Kate Cameron, Roger Lough, Emma Disley, Laurinda L. Rohn, Lucy Strang, Jonathan P. Wong

Prepared for the Department of Home Affairs and Australian Border Force

For more information on this publication, visit www.rand.org/t/RR2954

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0281-3

Published by the RAND Corporation, Santa Monica, Calif.

Preface

The Department of Home Affairs (hereafter referred to as the Department) and the Australian Border Force (ABF) are seeking to establish an auditable, transparent and evidence-based approach to a Capability Lifecycle Management Model (CLMM) that is flexible enough to meet the needs both of the Department and, potentially, of the Home Affairs Portfolio.[1] To accomplish that goal, in May 2018 the Department of Home Affairs and ABF Capability Review was initiated and RAND Australia was engaged to undertake a Capability Framework and Development Review.[2] The intent of RAND's review is to consider and critically evaluate the CLMM as a whole, and then formulate a detailed framework for the first four phases of the model (strategic planning, capability requirement, capability definition and investment decision).

To establish the maturity of the capability lifecycle management system within Home Affairs and to identify lessons, best practices, gaps and opportunities, RAND researchers conducted over 50 interviews with relevant Australian government officials, studied 14 capability development projects (both domestic and international), and undertook an extensive review of the key policy and capability development literature. The research team conducted interviews with and obtained key capability lifecycle documents from the Department, ABF, Victoria Police, Australian Department of Defence, the Department of the Prime Minister and Cabinet, UK Home Office, UK Cabinet Office, UK Ministry of Defence, U.S. Department of Homeland Security and U.S. Department of Defense. Based on our research, RAND developed a set of descriptions, characteristics and definitions related to the CLMM that have been tailored to the Home Affairs context.

In this report, the RAND researchers make 12 observations on the current approach to capability development within the Department and ABF. These led to a

[1] The Home Affairs Portfolio consists of the Department as well as a number of statutory agencies which may be governed under differing legislative arrangements and may utilise differing funding instruments. The five agencies within the Portfolio are the Australian Border Force, Australian Federal Police, Australian Criminal Intelligence Commission, Australian Security Intelligence Organisation and Australian Transaction Reports and Analysis Centre. See Australian Government, Department of Home Affairs, *Blueprint for Home Affairs*, 2018a, p. 9.

[2] Australian Government, Department of Home Affairs, *Terms of Reference – Home Affairs and ABF Capability Review (Draft)*, unpublished draft report, 2018f.

defined set of eight principles for the establishment and implementation of a CLMM, a detailed framework for strategic planning and capability requirements phases of the CLMM, and the identification of three options for governance models to support a future Home Affairs CLMM. The RAND team identified the need for a Capability Development function to support delivery of the CLMM. The report identifies a number of findings and posits 12 recommendations for consideration.

This research was sponsored by the Strategy and Capability Division within the Department of Home Affairs. Marc Ablong (Deputy Secretary Policy) and Mathew Fox (acting First Assistant Secretary, Strategy and Capability served as primary interlocutors with the RAND team and provided support to the study effort. This research was conducted within the Acquisition and Technology Policy Center of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the defense agencies, the Navy, the Marine Corps, the U.S. Coast Guard, the U.S. Intelligence Community, allied foreign governments, and foundations.

Comments or questions about this report should be addressed to the project leaders: Peter Dortmans (email: dortmans@rand.org) or Jennifer Moroney (email: moroney@rand.org). For questions regarding RAND Australia, please contact RAND Australia Director Carl Rhodes at crhodes@rand.org or 02 6232 6972.

For more information on the RAND Acquisition and Technology Policy Center, see www.rand.org/nsrd/ndri/centers/atp or contact the director (contact information is provided on the webpage).

Contents

Figures

Tables

Summary

On 20 December 2017, the Australian government established the Department of Home Affairs (hereafter referred to as 'the Department') with responsibility for policy, strategy, planning and coordination in relation to the domestic security and law enforcement functions of the Commonwealth, as well as managed migration and the movement of goods across Australia's borders. The Department forms a key part of the broader Home Affairs Portfolio,[1] which brings together Australia's federal law enforcement, national and transport security, criminal justice, emergency management, multicultural affairs, and immigration and border-related functions and agencies.[2]

In 2018, RAND Australia was engaged by the Department and the Australian Border Force (ABF) to develop a capability development framework suitable for their needs. In performing this task, the RAND research team examined the following study questions:

1. Which capability development lifecycle management framework best suits the needs of the Department for an enterprise-level approach to investment decisions?
2. How can best practices and lessons identified from similar organisations inform governance, policies, accountabilities, risk management and resource allocation within the strategy, planning and approval phases of the capability lifecycle management model?
3. What development path should Home Affairs follow to develop and maintain the knowledge, systems, practices and internal capabilities necessary for a sustainable and effective enterprise-level approach to investment approval?

[1] The Home Affairs Portfolio consists of the Department of Home Affairs as well as a number of statutory agencies which may be governed under differing legislative arrangements and may utilise differing funding instruments. The five agencies within the Portfolio are ABF, Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), Australian Security Intelligence Organisation (ASIO) and Australian Transaction Reports and Analysis Centre (AUSTRAC). In this report, when the term 'Portfolio' is capitalised it refers to this collection of government entities. See Australian Government, Department of Home Affairs, *Blueprint for Home Affairs*, 2018a, p. 9.

[2] See introductory remarks from Secretary Pezzullo in Parliament of Australia, *Legal and Constitutional Affairs Legislation Committee: Estimates, Department of Home Affairs*, 26 February 2018.

4. How might organisational and cultural issues associated with the newly established Home Affairs Portfolio be incorporated into capability-development lifecycle management?

Methodology

The methodological approach used by RAND is based on semistructured interviews with senior Department and ABF officials; interviews with relevant officials from other Australian government departments; interviews with people from similar organisations in the United Kingdom and the United States; a review of existing and emerging Department, ABF, and Portfolio strategies and policies; and related policies and supporting documentation from elsewhere in the Australian government and in existing academic literature.

The RAND Australia team conducted more than 50 semistructured interviews with senior Australian government officials. The RAND team was not able to engage with subject-matter experts (SMEs) from the other agencies within the Portfolio, as they were not available to meet with the team during the course of the analysis. As such, the report's findings are focused on meeting the needs of the Department and ABF. The team also reviewed a large number of policy and strategy documents.[3] The team undertook a thematic analysis to identify both Department and ABF needs and current capabilities in terms of capability development. RAND researchers then examined the capability development literature, as well as capability development approaches, employed by six Australian and international public sector organisations in order to identify lessons and best practice.[4] This review included eight international case studies. Analysis of these led to the establishment of design principles for capability development within Home Affairs, from which a capability development framework was created. The final phases of the methodology were to test the proposed model through eight workshops, each of which focused on an existing or previous capability-development project from within the Department (or its predecessor organisation).

[3] A number of key documents came out while this work was in progress. The RAND team reviewed these to ensure the analysis remained consistent with them.

[4] Specifically, RAND researchers examined the capability development frameworks employed by the Australian Department of Defence (Defence), Victoria Police, the U.S. Department of Homeland Security (DHS), the U.S. Department of Defense and the UK government.

Key Observations

The RAND team analysed the current needs for and practices in capability lifecycle management within Home Affairs, along with those of the practices of Australian and international peer organisations. The team identified a number of underlying issues that need to be considered when establishing a tailored approach to capability development. These issues are summarised as follows:[5]

- **Internal appetite for change:** There is an appetite among the senior Department and ABF staff to change to a strategy-centred approach for capability development and acquisition that incorporates a whole-of-life perspective, rather than focusing on the acquisition and operations phases.
- **Strategy-led:** Robust capability development requirements need to be clearly linked to capturing operational needs and traceable to strategic objectives.
- **Risk-versus-threat frame of reference:** There is a tension between those who favour pursuing a threat-based approach to capability development, which focuses on specific threats that tend to lead to investing in short-term solutions; and those favouring a risk-based treatment, who seek to design capabilities that meet enduring challenges.
- **Organisational patience:** Institutionalising a capability lifecycle approach across the Portfolio will take time, resources, and commitment from senior management, as it entails changes to governance, organisational culture, processes, and training and development.
- **Consistency improves quality:** The quality of capability decisionmaking is currently constrained by Home Affairs' lack of maturity and consistency in policies, frameworks and language.
- **Dedicated internal capability:** Successfully implementing a sustainable Capability Lifecycle Management Model (CLMM) requires an appropriate organisational structure, with capacity built around the competencies of permanent staff.
- **Phased rollout:** A phased rollout for implementation of the agreed approach is necessary to ensure that the Department can build internal competencies in capability development and project management.
- **Tailored governance:** Governance structures tailored to the complexity, size and risk of each program are required to give capability development programs greater agility and assurance.
- **Collaborative culture:** A more collaborative and collegial culture is needed between policy, acquisition, and operational staff at all levels as an essential prerequisite for establishing a resilient CLMM.
- **Building trust through transparency:** Home Affairs needs to develop and employ a robust and transparent process that incorporates all elements of the

[5] Further detail about these findings can be found in Chapter Two and Appendix D.

capability lifecycle to give the government the confidence it needs for capability investment approvals.
- **Forward-looking:** Local and international experiences demonstrate that robust research, development and innovation (RD&I) programs are essential for future-proofing Home Affairs, as such programs enable the exploration, acquisition and integration of new capabilities within dynamic environments.
- **Not a unique journey:** Peer organisations are also addressing this issue, with the UK Home Office and Home Affairs on a similar trajectory in developing and implementing a capability framework. The United Kingdom is slightly more advanced.

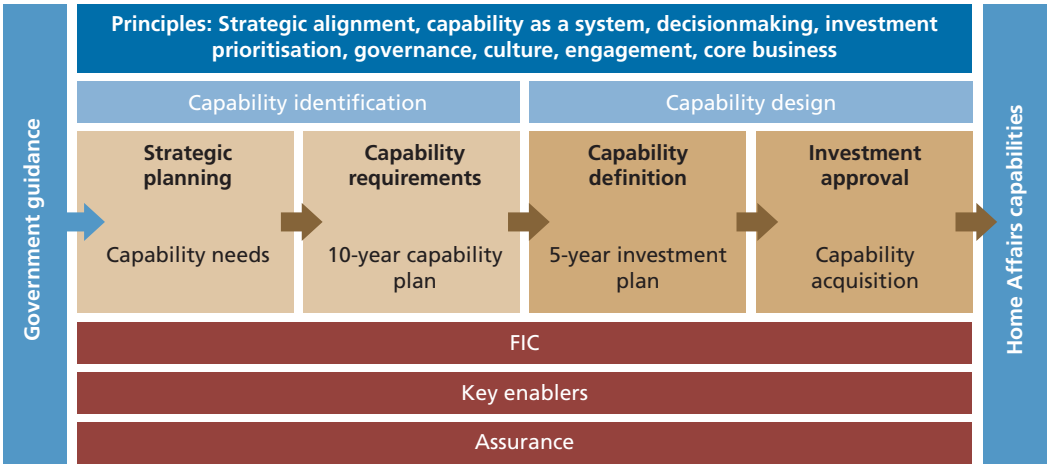
A Capability Development Framework for Home Affairs

For the purposes of this report, *capability* is defined as the capacity and intent to achieve and sustain a desired effect or output to meet one or more strategic objectives.[6] As such, an individual capability should be considered as a combination of elements that together represent the means to deliver the effect. From a Home Affairs perspective, examples of its existing capabilities would include the Future Maritime Surveillance Capability, the SmartGate system deployed at Australian airports, and the data warehousing system employed across the Department.

Based on this description of capability, and the findings and analysis conducted, the RAND team suggests that Home Affairs employ the capability development framework described in Figure S.1. The framework captures the essential elements required within a mature Home Affairs capability development system, namely, the translation of government guidance (on the left) into the acquisition of capability effects and outcomes (on the right). The premise is that the contributing elements that sit between these—and which are described below—will deliver the right mix of capabilities to meet Home Affairs' needs in a cost-effective and sustainable manner. At the core of the model are *capability identification* and *capability design*, which represent (respectively) the first and second, and third and fourth phases of the CLMM (shown in orange). While not explicit on the diagram, outcomes from each of the latter phases are fed back into the earlier ones. For instance, once an investment decision is made, both the capability plan and investment program would be updated to reflect any relevant changes. We note that the principles, Fundamental Inputs to Capability (FIC), key enablers, and assurance functions are relevant to all phases of the CLMM.

[6] Australian Government, Department of Home Affairs, *Terms of Reference – Home Affairs and ABF Capability Review (Draft)*, unpublished draft report, 2018f, p. 2.

Figure S.1
Capability Development Framework



Principles for Maturing the Capability Lifecycle

Based on our analysis, RAND identified eight overarching principles for maturing the capability lifecycle within Home Affairs:

1. **Strategic alignment:** Capabilities should be defined in terms of effects or outcomes that are traceable to strategic objectives, operational tasks and organisational functions.
2. **Capability as a system:** A capability is a system of interlocking and interdependent elements that, when combined, deliver one or more outcomes or effects. Capabilities should be grouped and partitioned into constructs that reflect department and agency missions that help enable effective program management.
3. **Decisionmaking:** Capability development decisions should be evidence-based, risk-informed, designed to accommodate emerging threats and opportunities, and incorporate interdependency implications. Staff need to be appropriately skilled,[7] empowered[8] and positioned within the organisation.[9]
4. **Investment prioritisation:** Capability investment should consider the entirety of the capability lifecycle, be prioritised in accordance with a strong evidence

[7] See Chapter Six for more detail.

[8] 'Empowered' entails ensuring staff are directly involved in the planning process to develop requirements from a frontline perspective.

[9] Appropriate organisational alignment has been found to be a key contributor to the success of capability development functions within government organisations.

base, and be internally contested at levels appropriate for its size, risk and complexity.

5. **Governance:** Capability development decisions should be made with accountability, transparency, integrity, stewardship, efficiency, effectiveness, leadership, teamwork and sustainability.[10] Decisions should be made with the involvement of a senior executive, a condition that demonstrates unity of purpose, an ownership of the decisions made, an understanding of the importance of taking appropriate risks, and a willingness to divest from capabilities as circumstances dictate. Timelines, key decision points, resources and interdependencies should be monitored throughout the capability lifecycle to ensure the capability development process is being managed effectively.
6. **Culture:** The organisation should embrace a collaborative culture that values intellectual honesty and transparency, encourages contesting and debating ideas when making decisions, accepts those decisions once they are made, and places the good of the enterprise over championing one's own organisational domain.
7. **Engagement:** Capability development decisions should be made in close consultation with relevant SMEs, and may benefit from close engagement with such experts as an integral part of the development process. Close consultation with all relevant Commonwealth, state and territory agencies, and international partners is a crucial component for the planning, development and utilisation of Home Affairs capabilities.
8. **Core business:** Home Affairs should seek to develop and deliver only those capabilities that cannot be delivered more effectively and efficiently by other entities.

Capability Development Phases

As the front end of the capability lifecycle, the capability development function is essential for ensuring informed acquisition decisions that meet the current and future strategic and operational needs of Home Affairs. Under this framework, the capability development system consists of two major activities, which cover the first four phases of the CLMM (displayed as the orange boxes in Figure S.1). These are the following:

- **Capability identification:** This activity uses government guidance to inform the development of a 10-year capability plan and includes the first two phases of the CLMM, namely,
  - **Strategic planning:** focusses on strategy and its role in informing and shaping capability development. It provides a risk-based view of the Department's present and future direction to inform forward planning of investment across

[10] See Appendix J for details on each of these terms.

the lifecycle of a capability, including acquisition, operations, sustainment and disposal of the inputs to that capability.[11]
  - **Capability requirements** are the points at which high-level capability gaps are identified, prioritised and endorsed. Capability proposals (incorporating capability needs statements and indicative budget provisions) are developed, and likely funding mechanisms identified.
- **Capability design:** This activity develops the acquisition strategy for each of the capabilities identified within the capability plan, and includes the third and fourth phases of the CLMM, namely,
  - **Capability definition:** encompasses the establishment of capability proposals, the development and exploration of options for addressing capability requirements, and the development of business cases to support prioritisation across a multiyear integrated investment program
  - **Investment approval:** transforms prioritised capability options into well-defined and costed solutions incorporating all FIC elements, which include whole-of-life workforce numbers and budgetary provisions to acquire, operate and sustain the capability solution.

Support Elements

Three key elements underpin the development of individual capability, namely, FIC, key enablers and assurance. The consideration of each of these elements, at each stage of the capability development lifecycle, will ensure the delivery of effects and outcomes in a cost-effective and sustainable manner.

Fundamental Inputs to Capability

As Principle 2 (*capability as a system*) notes, 'capability' is more than a platform and should be defined as the integration of contributing factors. In Australia, these are referred to as FIC. Analysis of domestic and international best practices emphasises the importance in treating capability as a system of contributing components, rather than as a physical product. As such, all peer organisations use a FIC construct. Based on our analysis of these, the RAND team recommends that Home Affairs use the following set of FIC and associated definitions:

- **People:** the appropriately sized workforce that has the necessary skills to perform the required role.
- **Training:** the education and skills development programs which enable the workforce to acquire and maintain appropriate skills and competencies.

[11] Best practice demonstrates that for strategic planning, a risk-based approach is preferred to a threat-based one. Threat-based approaches tend to focus on the operational and tactical challenges of the day, and so are less effective at supporting medium- to long-term capability planning. Our analysis of the experiences of peer organisations supports this premise.

- **Facilities:** the supply, development and maintenance of infrastructure required to effectively implement specific capabilities.[12]
- **Information and systems:** the reference and support materiel essential for the delivery of capabilities.[13]
- **Equipment and supplies:** the assets, hardware and materiel required to implement capabilities.
- **Support:** the operational and corporate services that underpin the capabilities, such as finance and maintenance support.
- **Laws, policies, procedures and administration:** ensuring that a capability incorporates all levels of required documentation and guidance.
- **Industry:** the capabilities of Australian industry, and the capacity of Australian businesses, to deliver not only operational and other capabilities, but the full spectrum of support functions.
- **Organisation:** the appropriate structures, personnel and balance of competencies to accomplish operational tasks and to ensure appropriate leadership, control and coordination.

Key Enablers

Key enablers are enterprise-level functions that support and contribute to the efficiency, effectiveness and sustainment of operational functions. They differ from FIC elements because key enablers are crosscutting and concurrently contribute to a number of functions and capabilities. Each enabler should be treated as a strategic asset, with its own enterprise-level plan and investment strategy that most effectively and efficiently invests the Department and ABF's finite resources into the right capabilities at the right time. The RAND analysis suggests that the key enablers for Home Affairs should include:

- **Capability development:** the function by which Home Affairs establishes, analyses and promotes its case for capability investment from government.
- **Information and communications technology (ICT):** the enterprise-level architecture and systems that underpin all Home Affairs capabilities.
- **RD&I:** the overarching strategy that future-proofs the organisation, capitalises on new opportunities and mitigates emerging threats.
- **Human resources (HR):** the strategic personnel plan that delivers the quantity and quality of people necessary to meet organisational demands while adhering to corporate and legal responsibilities.

---

[12] We note the emphasis on the support to the specific capability. As such, the broader critical infrastructure needs are considered separately as a key enabler.

[13] As is the case for Defence, ICT is an important and strategic asset for the Portfolio (see Australian Government, Department of Defence, *2016 Defence White Paper*, 2016a, p. 84).

- **Strategic budgeting:** the capacity to develop budget forecasts that inform enterprise-level planning across all relevant time frames.
- **Critical infrastructure and estate management:** the estates and physical infrastructure necessary to support the delivery of all functions across the enterprise.
- **State and territory engagement:** the provision of national-level coordination across key Home Affairs domains, through strategic and operational relationships with domestic partners.
- **International partnerships:** strategic collaborative arrangements with international peers to enhance the capabilities of Home Affairs and its regional partners, and to be a conduit for domestic partners.

Assurance and Contestability

The overarching policy for ensuring good governance by Australian government entities is the Public Governance, Performance, and Accountability Act (PGPA).[14] While the PGPA provides the basis for external assurance and scrutiny, it assumes these functions are built upon existing internal processes that ensure Home Affairs makes robust and informed investment decisions. The application of a governance model that practices contestability across all capability development phases is key to internal assurance and scrutiny. The expectation for contestability can be seen by an Australian National Audit Office (ANAO) report that found a structured program for contestability 'was effective in supporting entities to review the efficient and effective delivery of government functions'.[15] However, incorporating a contestability function into Home Affairs will have resource implications, so it will be necessary to develop an appropriately tailored contestability framework.

Governance Options

The way in which this framework will be employed by Home Affairs will largely be contingent on the level of centralisation of the capability development function within the Department, ABF and the other Portfolio agencies. While RAND does not make any specific recommendations about the governance model that should be employed by Home Affairs, it identifies three models that could be employed, with the key attributes of each model examined. The three models, based upon responsibilities within the capability development function, are the following:

- **Centralised governance:** where responsibility for the four capability development phases of the CLMM resides with a single entity within the Department.

---

[14] Australian Government, Department of Finance, *Public Governance, Performance and Accountability Act 2013*, 2019.

[15] ANAO, "Efficiency Through Contestability Programme," webpage, 20 May 2018a.

The remaining three phases of the CLMM are delivered by a separate organisational entity.

- **Semicentralised governance:** where the strategic planning phase is provided by one entity within the Department. All of the remaining capability development phases and follow-on phases are delivered by a separate entity within the Department.
- **Decentralised governance:** where the Portfolio agencies develop, deliver and sustain their own capabilities.

These models should not be considered in isolation and could be combined, if required.[16] It is also recommended that governance structures are tailored in accordance with the complexity, size and risk of each program. Incumbent within each model is the need to develop a dedicated and enduring capability development function to support these that is organisationally separate.

The employment of a risk-based approach to determining the level of governance required for a program would give the programs within Home Affairs greater agility and assurance. Initially, Home Affairs could tailor its governance structure in accordance with the complexity, size and indicative risk of each program until a mature risk framework can be developed.

Building the Capability Development Function

Finally, this analysis considered the key skills, knowledge and competencies required for the capability development team. The analysis showed that a diverse range of skills is required, with a likely substantial increase in the number of staff allocated to the capability development function. A more detailed analysis of the size and structure of the team should be considered as key decisions are made within the Department and the Home Affairs Portfolio about the level of centralisation of the capability development function.

It should be noted that this report represents one of a number of reviews concurrently being undertaken by the Department and ABF that consider components of the Home Affairs capability development system. While the RAND Australia team sought information about the findings of other concurrent reviews, these findings were often interim in nature. While it is likely that the findings from the other reviews will focus on other aspects of the capability development lifecycle, the final findings of all reviews should be considered in unison to ensure consistency and applicability of findings across each of the internal reviews.

[16] Further detail is provided in Chapter Five and Appendix K.

Recommendations

Based on these findings and analysis conducted to establish best practice in capability development, the RAND team makes the following recommendations:

Recommendation 1: Employ the capability development framework described in Figure S.1. This framework captures the essential activities required within a mature Home Affairs capability development system, namely the translation of government guidance into capabilities that deliver the required effects and outcomes in a cost-effective and sustainable manner (Chapter Three).

Recommendation 2: Use the eight overarching principles for capability development within Home Affairs identified within this report. These principles focus on strategic alignment, a systems perspective of capability, decisionmaking, investment prioritisation, governance, organisational culture, internal and external engagement, and core business focus (Chapter Three).

Recommendation 3: Adjust Home Affairs' current FIC model by adding industry and organisation to the current set of inputs (people training; facilities; information and systems; equipment and supplies; support; and laws, policies, procedures and administration) and use the definitions outlined in the report (Chapter Three).

Recommendation 4: Treat key enabling functions as strategic resources and explicitly incorporate investment decisions associated with these functions when establishing the integrated investment program. At a minimum, the key enablers that should be included are capability development; ICT; RD&I; HR; strategic budgeting; critical infrastructure and estate management; state and territory engagement; and international partnerships (Chapter Three).

Recommendation 5: Consider an organisational structure that aligns with the two major activities of the capability development phases of the CLMM: capability identification and capability design (Chapter Four).

Recommendation 6: Incorporate the capability development approach into its corporate planning cycle, develop a 10-year capability plan, develop a 5-year integrated investment program, and use these plans to support capability investment decisions (Chapter Four).

Recommendation 7: Employ the interim logic models for capability identification, with the aspiration to transition to the mature model in the future (Chapter Four).

Recommendation 8: Employ the logic models for capability design in order to develop robust, evidence-based acquisition business cases that are adapted to project complexity (Chapter Four).

Recommendation 9: Recognise the key role SMEs perform throughout the capability development process, and invest resources to ensure their ongoing availability to those responsible for the capability development function (Chapter Four).

Recommendation 10: Choose the governance model that best suits Home Affairs circumstances; establish the necessary knowledge, systems and organisational structures to support it; and empower and resource the key stakeholders appropriately (Chapter Five).

Recommendation 11: Establish and resource a capability development function (Chapter Six).

Recommendation 12: Develop a detailed implementation plan for institutionalising capability development (Chapter Seven).

Taken together, these recommendations establish a basis for the implementing the proposed capability development approach. Clearly, implementation is contingent on approval by the senior executive committee. Once the decisions associated with the capability development model are made, including the choice of governance model, actions can be taken to make the structural changes necessary. The development of the detailed implementation plan would be shaped by the strategy for applying it across Home Affairs. Given that the proposed CLMM model represents a major change to how Home Affairs currently operates, we anticipate that a phased rollout of an implementation plan would be suitable to facilitate organisational learning and process improvement, while minimising disruptions.

Acknowledgements

We would like to thank the following members of the Department of Home Affairs project team for their continuous interaction and guidance: Marc Ablong, Mathew Fox, Carrie Coleman, Laura Long, Andrew Tarte, Phillip McDougall and William McClure. We would also like to thank the many representatives of the Department of Home Affairs, the Australian Border Force, and other government officials from Australia and the United Kingdom, as well as a number of RAND subject-matter experts from the Homeland Security Operational Analysis Center (HSOAC),[1] who were willing to talk to or meet with us. These representatives included:

- Department of Home Affairs: Vanessa Bajt, Ryan Balthazaar, Jennifer Bardsley, Leanne Blackley, Abigail Bradshaw, Andrew Brennan, Tom Bryan, Sally Buik, Stephanie Cargill, Jeff Carige, Pablo Carpay, Kylie Coghill, Renate Crocker, Kerri Dalla, Heidi Djokic, Martin Dunn, Belinda Duffy, Carol Estereich, Bill Eversham, Kristina Faigl, Maria Fernandez, Linda Geddes, Malisa Golightly, Rhys Goodwin, David Graham, Richard Gray, Paul Grigson, Aled Hall, Lisa Harris, Sean Hugo, Nicholas Jeans, Tyna Keane, Andrew Kefford, Karl Kent, Radi Kovacevic, Tony Kummer, David Leonard, Alastair MacGibbon, Luke Mansfield, Nathaniel Maras, Michael Milford, Sue Miller, Freddie Minson, Cheryl-Anne Moy, Nigel Muir, David Nockels, Bret O'Neill, Andrew Rice, Peter Richards, Danielle Robinson, Tony Sheehan, Felicity Smart, Duane Smith, Gemma Smyth, Ciara Spencer, Ruth Williams, Sachi Wimmer, Patrick Winters and Barbara Wooderson.
- Australian Border Force: Assistant Commissioner Victoria Holben, Brendan Kosmer, Deputy Commissioner Mandy Newton, Commissioner Michael Outram, Assistant Commissioner Clive Murray, Fatime Shyqyr and Assistant Commissioner Kingsley Woodford-Smith.
- Other Australian federal and state government departments: Brigadier Jason Blain, Darren Coonan, Alison Creighton, Patrick Hetherington, Ciril Karo, Rear

[1] HSOAC is a federally funded research and development center operated by the RAND Corporation, under contract with the DHS.

Admiral Stuart Mayer, Gareth Sebar, Assistant Commissioner Neville Taylor, John Toohey, Chad Tyrell, Anthony Ween and Georgia Williams.

- UK government officials, including a representative from the UK Cabinet Office, responsible for the capability mapping programme; a representative from UK Defence Science and Technology Laboratory responsible for establishing a commissioning hub; and two interviews with a total of six senior officials in the UK Home Office, who worked on the development of a strategic planning framework.[2]
- U.S. subject-matter experts: two representatives from U.S. Department of Homeland Security and six representatives from HSOAC.

We thank Irv Blickstein, Joseph Chang, Carl Rhodes, Dan Gerstein, Angela Putney, Anita Chandra and James Anderson for their thoughtful reviews of this report, and Gordon Lee for his great work on this report as our communications analyst.

---

2 UK and U.S. officials were spoken with on the basis of nonattribution.

Abbreviations

ABF	Australian Border Force
ACAT	acquisition category
ACIC	Australian Criminal Intelligence Commission
ACTD	Advanced Concepts Technology Demonstrator
AFP	Australian Federal Police
AMO	Air and Maritime Operations
ANAO	Australian National Audit Office
AoA	analysis of alternatives
APSC	Australian Public Service Commission
ARB	Acquisition Review Board
ASIO	Australian Security Intelligence Organisation
AUSTRAC	Australian Transaction Reports and Analysis Center
BoI	balance of investment
BRACS	Budgeting, Reporting and Costing System
CASG	Australian Capability Acquisition and Sustainment Group
CAST	UK Centre for Applied Science and Technology
CBP	capability-based planning
CFDR	capability framework and development review
CGA	capability gap assessment
CIA	U.S. Central Intelligence Agency
CIO	chief information officer
CLMM	Capability Lifecycle Management Model
CM	capability manager
CPRSC	Capability Planning and Resources Steering Committee
DARPA	U.S. Defense Advanced Research Projects Agency
DCB	Department Capital Budget

DCP	Defence Capability Plan
DCGS-A	Distributed Common Ground Sensor—Army
DIBP	Australian Department of Immigration and Border Protection
DHS	U.S. Department of Homeland Security
DMAG	U.S. Deputy's Management Action Group
DoD	U.S. Department of Defense
DST Group	Australian Defence Science and Technology Group
Dstl	UK Defence Science and Technology Laboratory
FDD	Force Design Division
FIC	fundamental inputs to capability
FY	financial year
GA-ASI	General Atomics Aeronautical Systems, Inc.
GAO	U.S. Government Accountability Office (formerly General Accounting Office)
GCS	ground control station
GFE	government-furnished equipment
HR	human resources
HSOAC	Homeland Security Operational Analysis Centre
ICT	information and communication technology
IP	intellectual property
ISR	intelligence, surveillance and reconnaissance
JAR	joint assessment of requirements
JCIDS	Joint Capability Integration and Development System
JRC	Joint Requirements Council
JRIMS	Joint Requirements Integration and Management System
JROC	Joint Requirements Oversight Council
NPOC	net personal and operating costs
NPP	New Policy Proposal
MoD	UK Ministry of Defence
PGPA	Public Governance, Performance and Accountability Act
PM&C	Department of the Prime Minister and Cabinet (Australia)
R3	Review and Reinvestment Roadmap
RACI	responsible, accountable, consulted, informed

RAG	red, amber, green
RCP	Resilience Capabilities Programme
RD&I	research, development and innovation
S&T	science and technology
SCD	Strategy and Capability Division
SES	Senior Executive Staff (Australia)
SMART	specific, measurable, assignable, realistic, time-related
SME	subject-matter expert
SOCOM	Special Operations Command
SPF	strategic planning framework
UAV	unmanned aerial vehicle
UKHO	United Kingdom Home Office
USCG	United States Coast Guard
VCDF	Vice Chief of the Defence Force (Australia)

CHAPTER ONE

Introduction

Background

On 20 December 2017, the Australian government established the Department of Home Affairs (hereafter referred to as 'the Department'), with responsibility for policy, strategy, planning, and coordination in relation to the domestic security and law enforcement functions of the Commonwealth, as well as managed migration and the movement of goods across Australia's borders.

The Department forms a key part of the broader Home Affairs Portfolio,[1] which brings together Australia's federal law enforcement, national and transport security, criminal justice, emergency management, multicultural affairs, and immigration and border-related functions and agencies.[2] The government's intent is that this larger and more integrated Portfolio will be better equipped to build more holistic capabilities, by leveraging the capabilities that already exist in its component parts.[3] The systems employed within the Department are critical national infrastructure, the failure of which has significant and visible impacts on Australia's security and prosperity.[4] The

[1] The Home Affairs Portfolio consists of the Department of Home Affairs, as well as a number of statutory agencies which may be governed under differing legislative arrangements and may utilise differing funding instruments. The five agencies within the Portfolio are the Australian Border Force (ABF), Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), Australian Security Intelligence Organisation (ASIO), and Australian Transaction Reports and Analysis Centre (AUSTRAC). In this report, when the term 'Portfolio' is capitalised, it refers to this collection of government entities. See Australian Government, Department of Home Affairs, *Blueprint for Home Affairs*, 2018a, p. 9.

[2] See introductory remarks from Secretary Pezzullo in Parliament of Australia, *Legal and Constitutional Affairs Legislation Committee: Estimates, Department of Home Affairs*, 26 February 2018.

[3] See Minister Peter Dutton, "Address to the National Press Club of Australia, Canberra," speech delivered at the National Press Club, 21 February 2018.

[4] Australian Government, Department of Immigration and Border Protection (DIPB), *Technology Review*, internal document, 2016, p. 2.

Department is unique for having an operationally focused portfolio because it is the second-largest collector of revenue for the Australian government.[5]

The successful development and implementation of a coherent capability development framework are important drivers for establishing the strategic direction of the Home Affairs Portfolio. The Department and ABF have initiated a program of work aimed at establishing a more robust Capability Lifecycle Management Model (CLMM) for their areas of responsibility. To this end, they have initiated the Department of Home Affairs and ABF Capability Review (hereafter referred to as the Capability Review).[6] The review consists of the following three components, the second of which is the subject of this report:[7]

- **Capability Baseline Review:** an assessment of current ABF capability.
- **Capability Framework and Development Review (CFDR)**: phases 1–4 of the CLMM, the development of a framework from strategic planning through to investment approval.
- **Capability Delivery and Management Review (operations and sustainment)**: phases 5–7 of the CLMM, the development of a framework for capability acquisition through life support and disposal.

Purpose

This report is intended to provide the Department and ABF with the details necessary to establish best practice in capability development. Best practice is achieved through a principles-based model that identifies an overarching framework, mechanisms, processes, governance arrangements and internal capabilities for capability development. Further, there are a number of reviews running concurrently within the Home Affairs Portfolio that are related to the capability lifecycle. This project is one of three activities being undertaken under the Capability Review. This report will allow the Department and ABF to ensure alignment between all elements of the Capability Review and the other major reviews within the Portfolio. Further, there are a number of stakeholders within the Department and ABF (and potentially across the Portfolio) that will be affected by the implementation of a capability framework.

---

5 ABF, *ABF 2020*, 2016, p. 14.

6 Australian Government, Department of Home Affairs, *Terms of Reference – Home Affairs and ABF Capability Review (Draft)*, unpublished draft report, 2018f.

7 The Capability Baseline Review and Capability Delivery and Management Review were undertaken by another commercial entity, and are considered in this report.

Study Outline

RAND Australia was engaged to undertake the CFDR by developing an auditable, transparent and evidence-based approach to capability development, tailored to the needs of the Department and ABF (see Appendix A). The study's aim has been to develop a detailed framework that defines and connects capability identification (strategic planning and capability requirements) with capability design (capability definition and investment approval).[8] Based on the terms of reference, the RAND research team examined the following study questions:

1. Which capability development lifecycle management framework best suits the needs of the Department for an enterprise-level approach to investment decisions?
2. How can best practices and lessons identified from similar organisations inform governance, policies, accountabilities, risk management and resource allocation within the strategy, planning and approval phases of the capability lifecycle management model?
3. Which development path should Home Affairs follow to develop and maintain the knowledge, systems, practices and internal capabilities necessary for a sustainable and effective enterprise-level approach to investment approval?
4. How might organisational and cultural issues, associated with the newly established Home Affairs Portfolio, be incorporated into capability development lifecycle management?

Initial discussions with the Department's officials who commissioned this study and analysis of these questions identified four key study requirements, namely,

- an overarching capability development framework and taxonomy
- the creation of governance approaches and enabling capabilities to support the framework and taxonomy
- using logic models and associated processes to enable capability development processes to be conducted in a consistent and transparent manner
- taking steps that enable the model's successful implementation.

A research methodology was established (see Appendix B). It was based upon semistructured interviews with senior Department and ABF officials; interviews with relevant officials from other Australian government departments; interviews with people from similar organisations in the United Kingdom and United States; a review of existing and emerging Department, ABF and Portfolio strategies and policies; and

[8] These terms are described in more detail in Chapter Four.

related policies and supporting documentation from elsewhere in the Australian government, and in existing academic literature.

The RAND Australia team conducted more than 50 semistructured interviews with senior Australian government officials. It also reviewed a large number of policy and strategy documents. A thematic analysis was undertaken to identify both the Department and ABF needs and current capability in terms of capability development. RAND researchers then examined the capability development literature, as well as capability development approaches employed by five Australian and international public sector organisations,[9] in order to identify lessons and best practices. Eight international case studies were included. Analysis of these led to the establishment of design principles for capability development within the Department, from which a capability development framework emerged. The final phases of the methodology were to test the viability of the proposed model through eight workshops, each of which focused on an existing or previous capability project from within the Department and ABF (or its predecessor organisation). The outcomes of these were used to refine the model.

The outcome of the analysis has led to the establishment of a capability development framework tailored to the needs of the Department and ABF.[10] These needs, processes, and the team's recommendations are outlined in the remainder of the report, as follows:

- capability development, as it is currently practised in the Department, and lessons identified from international and domestic experiences (Chapter Two)
- a capability development framework, including recommended definitions, principles and criteria for capability development within the Department (Chapter Three)
- the logic models and processes by which capability is defined and matures across the capability-development phases of the CLMM (Chapter Four)
- potential governance models to support capability development (Chapter Five)
- the establishment and implementation of the capability development phases of the CLMM, including the enabling Capability Development function (Chapter Six)
- recommendations based upon our analysis (Chapter Seven)
- twelve appendixes that provide more details about the information covered within the main body of the document.

Each chapter represents one of the four study requirements identified above. While the report is structured to separate these, it should not be treated as a chrono-

[9] Specifically, RAND researchers examined the capability development frameworks employed by the Australian Department of Defence (Defence), the Victoria (Australia) Police, the U.S. Department of Homeland Security (DHS), the U.S. Department of Defense (DoD), and the UK government.

[10] Throughout the analysis, consideration was given to enabling a straightforward extension across the Portfolio.

logical account, with each chapter building on the previous one; it should be read as a manual, where each chapter has dependencies on all other chapters.

Assumptions and Limitations

It should be noted that this report's findings are subject to a number of assumptions and limitations. These include the following:

- The RAND team was only able to engage with Department and ABF staff; subject-matter experts (SMEs) from other agencies within the Portfolio were not available to meet with the team during the course of this analysis. As such, the report's findings are intended to meet the needs of the Department and ABF, based on feedback provided to the study team. While the team has tried to include considerations for the broader Portfolio, their larger applicability should be developed in consultation with SMEs from the relevant Portfolio agencies.
- As noted earlier, this report represents one of a number of reviews concurrently being undertaken by the Department and ABF that consider components of the Home Affairs capability development system. While the RAND team sought information about the findings of other concurrent reviews, these findings were often interim in nature. While it is likely that findings from the other reviews will focus on other aspects of the capability development lifecycle (e.g., the length of the capability plan or investment program), the final findings of all reviews should be considered in unison to ensure consistency and applicability of findings, across each of the reviews.
- Information for some case studies was not available in published reports; in those instances, the RAND team relied upon a small number of interviews. In addition, some case studies reported on developments that are in progress. As a result, verification was difficult, therefore the lessons inferred from these developments should be considered promising rather than proven practice.

CHAPTER TWO

Current Capability Development Practices

In this chapter, we examine the current capability development framework within the Department and ABF and compare these practices with those used in similar domestic and international public sector organisations.

The Department of Home Affairs

Establishing the requirements for and needs of the Department and ABF in capability design, development, acquisition and management was a critical first step in the RAND team's effort to develop the capability framework for the CLMM. The research team achieved this through a combination of semistructured interviews and a review of strategy and policy documents, as well as select Portfolio and project documentation.

Blueprint and Corporate Plan

In July 2018, the Home Affairs Portfolio released its Blueprint.[1] This represented the first time that the new Portfolio articulated, in a cohesive manner, what its strategic aims were, the responsibilities of each entity, how these were to be achieved by the Department and Portfolio agencies, and the relationships between these previously separated entities since the establishment of the Department in December 2017. In effect, this established the strategic baseline for the organisation and highlighted the need for an integrated approach to acquiring and maintaining capability.

The Blueprint casts the Portfolio's strategic objectives around the following three broad outcomes:

- **Prosperous:** focuses on its contribution to 'Australia's prosperity by enabling a globally connected and open economy and society'
- **Secure:** focuses on protecting 'Australia and Australians from key national security and criminal threats'

[1] Australian Government, Department of Home Affairs, 2018a.

- **United:** focuses on 'building community resilience and engendering respect for Australia's shared values and institutions, our way of life and the rule of law'.[2]

To achieve these objectives, the Blueprint expects Home Affairs to be 'strategy-centred and led', seeking to 'deliver a holistic, strategic picture of the threat environment, identify options to mitigate threats and further our national interests', and 'implement … existing national strategies'.[3] The Blueprint articulates a future state where, among other things, the Portfolio culture is one of innovation that is built around 'the use of technology to support our staff, achieve our mission and deliver government objectives' and which employs 'agile and adaptive business processes that embrace management of risk and empower decision-making'.[4] The Blueprint is also seeking 'greater transparency of committee decisions'.[5]

In September 2018, the Department released its first Corporate Plan, which states that 'the newly integrated functions of the Department will require fit-for-purpose capabilities—the capacity and ability to achieve and sustain a desired outcome. Capabilities depend on fundamental inputs, including people, legislation, policy, facilities, information and systems, procedures and administrative support, equipment and supplies, and training. The Department will continue to develop and implement capability initiatives that enable us to be resilient, flexible, innovative and efficient. Astute and well-planned capability investments allow us to be more responsive to new challenges and to the requirements of Government and key stakeholders.'[6]

The Corporate Plan goes on to define capability planning as 'an assessment of the Department's and ABF's strategic priorities and risks, and identification of capability gaps. This helps to determine what investments in future capability are required and when they are needed.'[7] The intention is to 'develop and implement an efficient, integrated, enterprise-level operating model across the capability lifecycle. Capability planning will determine the Department's investment priorities for the next five to ten years … [through] a strong alignment between our strategic objectives and investment, ensuring that we can deliver robust, value-for-money, effects-based, forward-looking capabilities, transforming our systems, processes and technology while maintaining business-as-usual activities.'[8]

---

2 Australian Government, Department of Home Affairs, 2018a, p. 11.

3 Australian Government, Department of Home Affairs, 2018a, p. 27.

4 Australian Government, Department of Home Affairs, 2018a, p. 33.

5 Australian Government, Department of Home Affairs, 2018a, p. 39.

6 Australian Government, Department of Home Affairs, *Corporate Plan 2018–19*, 2018b, p. 19.

7 Australian Government, Department of Home Affairs, 2018b, p. 19.

8 Australian Government, Department of Home Affairs, 2018b, p. 19.

Taken together, the Blueprint and Corporate Plan establish the strategic basis for capability development within the Department; namely, that capability development is strategy-led and risk-based, that it is able to balance current and future needs, that it allows decisionmakers to determine the optimal set of capabilities given the budgetary environment, that it takes a portfolio and enterprise view, and that the entirety of the capability lifecycle is considered. We note that while these key documents came out as this work was in progress, and after the model development had commenced, they were consistent with the guidance provided to the RAND team in discussions with the Department.

Current Capability Lifecycle Model

The Capability Review Terms of Reference stipulated that the Department and ABF employ a seven-step CLMM (see Figure 2.1).[9] The CLMM is based upon a previous attempt by the DIBP to establish a CLMM.[10] The RAND team has been advised that while the seven phases were endorsed by the DIBP Executive, the approach, as proposed, was not. As the model depicted in Figure 2.1 is consistent with the international standard for asset management,[11] and with approaches others have taken in capability lifecycle management, the research team does not propose altering the model. However, the RAND team makes recommendations for what defines each step (see Chapter Three), namely the following:

- Strategic Planning, the first stage, focuses on strategy and its role in informing and shaping capability development. It provides a view of the Department's present and future direction to inform forward planning of operational and capital investment;
- Capability Requirements is the point at which high-level capability gaps are identified, and proposals are reviewed and prioritised for funding, either externally via a New Policy Proposal or internally through the Departmental Capital Budget;
- Capability Definition encompasses the development of business cases to support prioritisation of proposals only seeking external funding;
- The Investment Approval stage involves the preparation of New Policy Proposals and associated Cabinet submissions. Funding associated with proposals is considered by Government as part of the budget process;

---

[9] Australian Government, Department of Home Affairs, 2018f, Annex B. We note that the documents provided have had minor variations of this, particularly with respect to the naming conventions for phase 6—Capability Operation and Sustainment.

[10] Note that the focus of this report is the initial four phases of the CLMM, represented in blue in Figure 2.1.

[11] International Organization for Standardization, "Asset Management—Overview, Principles and Technology," ISO 55000:2014(en), 2014.

- The Capability Delivery stage is focused upon acquisition/development of capability with an eye on the downstream in-service management (sustainment) and subsequent disposal and documented in the Post Investment Procedural Instruction;
- The Capability [Operation and] Sustainment stage covers the requirement for the Capability Owner to monitor the various enabling elements and undertake continual needs and requirements analysis to ensure that the acquired capability remains strategically relevant and fit for purpose; and
- The Capability Disposal stage provides for the planned withdrawal of a capability at the end of its useful life. This phase is significant as early identification of the planned withdrawal date initiates action in the Capability Requirements stage to plan for a replacement or follow-on system.'[12]

It should be noted that this report will primarily focus on the development of a framework for the first four phases of the CLMM for the Department and ABF (the blue boxes in Figure 2.1), set within the context of the entirety of the CLMM. The details of how the CLMM framework is implemented depend on the approach chosen and should be the focus of follow-on analysis. As such, implementation of the CLMM is outside of the scope of this work.

Internal Perceptions of Capability Development

Building on the strategies and policies outlined previously, and to gain a better understanding of capability development as it is practised within the Department and ABF, RAND researchers conducted 52 semistructured interviews of 74 individuals, both within and outside of the Department and ABF (see Appendix B).[13] Of these interviews, 57 officials from within the Department and ABF were engaged across 33 interviews, of whom 22 were at the First Assistant Secretary or Deputy Commissioner level and above.

Figure 2.1
Current Home Affairs Capability Lifecycle Management Model

[12] Australian Government, DIPB, *Capability Management*, unpublished presentation, 2017b.

[13] These interviews were mostly face-to-face, with three interviews taking place over the telephone.

Table 2.1
Key Issues Raised in Interviews

Frequency Raised	Issues
High	• Lack of a long-term, enterprise planning approach for capability planning and development • Lack of a suitable governance structure to support capability lifecycle management • Lack of a 'golden thread' of logic that links investment to strategy • Organisational structure and culture tend to inhibit progress, rather than enable it • Lack of capacity and experience in capability development
Medium	• Current funding model cannot deliver long-term capability needs • Tendency to focus on immediate threats, rather than positioning for future challenges and opportunities • Need to tailor the capability lifecycle model to be a scalable, enterprise approach • Lack of an effective prioritisation approach to support investment and divestment decisions • Difficulty in delivering effective quality assurance and contestability functions • Failure to plan and resource capabilities beyond their acquisition • Failure to recognise key enablers as strategic assets that require investment • Inconsistent understanding of capability
Low	• Tendency for replacement of capabilities rather than exploring new options • Need for more strategic engagement with central agencies and government • Capability requirements are not understood in a structured manner • Need to engage industry early • Need to recognise agency-specific statutory constraints

Having undertaken an analysis of those interviews, the research team identified 19 key issues, characterised as representative statements,[14] as shown in Table 2.1 (see Appendix C for more details). These statements, weighted against the regularity of their occurrence, capture the needs for and perceive current gaps within the capability development process. As such, they form an important component of the design criteria for the model.

Australian Public Sector Organisations

Capability development in the Australian public sector has a long history. Given the current capability development practices within the Department, the project researchers elected to explore, in detail, policies and case studies that address particular challenges or issues for the Department. RAND researchers reviewed the Department's practice in Australia in order to identify lessons and best practices. Specifically, the research team focused on two examples of CLMM implemented within the Australian National Security sector: Defence, which embraced a capability development process some time ago, and the Victoria Police, which implemented CLMM more recently.

[14] We note that the categorisation is not orthogonal, as there are overlaps between the issues.

Defence Approach to the Capability Lifecycle

Defence, like defence departments in the countries of many of Australia's allies, has employed holistic capability development frameworks in one form or another for many years.[15] Its approach represents the most aligned of all the approaches that the RAND researchers considered, as Defence and the Department both encounter the same environment for investment approval, governance and reporting. This section covers the key insights that the RAND team discovered; for a detailed description of the Defence CLMM, readers should turn to Appendix D.

Defence has defined *capability development* as the ability to 'develop and maintain the most operationally effective and cost-efficient mix of capabilities required to achieve [the g]overnment's strategic objectives.'[16] Here, *capability* is defined in terms of effects or outcomes, and is constituted through the integration of various materiel and nonmateriel inputs.

The strategic basis for all Defence capability development is the Defence White Paper, an articulation of the 'government's broad strategic objectives and the capabilities needed for them to be achieved within fiscally responsible and realistic boundaries'.[17] The criticality of the Defence White Paper was emphasised by one of the senior Defence officials interviewed as a contract with government, which provided a common aim point for capability planning and the underlying value proposition for justifying investment across the Defence Portfolio. Through the White Paper, Defence is given clear direction as to how and where it is expected to contribute domestically and globally, allowing it to develop a long-term capability plan that prioritises capabilities choices.[18] It also provides the basis for the way in which the government assesses its performance, by clearly articulating strategic objectives and principal tasks. It should be noted that, although the White Paper provides the strategic guidance for the capability development process, subordinate strategies are also required to define the more detailed requirements of the capabilities listed within the White Paper.[19]

Under Defence's approach, capability is considered a continuum and is managed that way. Each individual capability has a lifecycle that begins with 'the development of a simple statement of user need that is developed into a capability solution for acquisition, introduction into service, operation and sustainment [and] is completed with

---

15 Australian Government, Department of Defence, *First Principles Review: Creating One Defence*, 2015, p. 13.

16 Australian Government, Department of Defence, *Defence Capability Development Handbook 2012*, 2012a, p. 5.

17 Nicole Brangwin, Nathan Church, Steve Dyer, and David Watt, *Defending Australia: A History of Australia's Defence White Papers*, Australian Parliamentary Library, August 20, 2015.

18 Hugh White, "Strategic Interests in Australian Defence Policy: Some Historical and Methodological Reflections," *Security Challenges*, Vol. 4, No. 2, Winter 2008, pp. 63–79.

19 Referred to as 'tier-two strategies' within Home Affairs.

disposal'.[20] Given the complexity of the Defence enterprise and the capabilities that underpin it, the capability lifecycle requires a forward-looking, portfolio perspective. This is captured though a 10-plus-year capability plan to link strategic guidance to capability, engender informed long-term planning, and ensure the efficient and effective delivery and sustainment of an optimal defence portfolio. Defence breaks the capability lifecycle into two distinct phases, the *Needs Phase*, which focuses on the strategy, capability requirements and investment decisions processes; and the *Acquisition Phase*, which focuses on acquisition, sustainment and disposal.[21]

While the Defence approach has (and continues) to evolve, there are some key enduring principles which are considered to be best practices. These include[22]

- discipline in the application of the CLMM
- real choice in the capability options offered to the government; timeliness that allows considered decisionmaking
- a whole-of-government perspective to encourage interoperability and avoid stovepiping
- collaboration and transparency that builds confidence with government
- executable and sustainable capability proposals that can be delivered within scope, schedule, budget and workforce allocations, and sustained within resource boundaries
- risk-informed proposals that allow the government to understand the consequences of its decisions
- demonstrable value for money built on sound cost-benefit analysis
- documentation of decisions that allows for transparency, with future decisionmakers understanding the basis of the original decision
- appropriate levels of accountability and scrutiny.

Defence has employed different approaches to seeking government approval. Prior to the recent *Force Principles Review*, it used a two-pass process for government approval for most capability projects, with the first-pass approval focusing on capability gaps and broad (diverse) options for addressing them, and the second-pass approval seeking investment approval for the chosen capabilities. At both passes, it was expected that a robust evidence base would be available to inform decisions. In recognition that capability projects have differing levels of complexity, the two-pass approach was adapted to accommodate this. Projects assessed as low complexity could forgo first-pass approval, while highly complex projects might require additional passes that sup-

[20] Australian Government, Department of Defence, 2012a, p. 4.

[21] Australian Government, Department of Defence, 2012a, p. 4.

[22] Australian Government, Department of Defence, 2012a, p. 5.

port a more incremental process.[23] It should be noted that under this new approach, the basic phases of strategy, capability requirements and definition, acquisition, operations, sustainment and disposal remain.

Notwithstanding this, the *First Principles Review* found that Defence processes were complicated, slow and inefficient; there was uncertainty over accountabilities and responsibilities at senior levels; there was unnecessary escalation of issues to senior decisionmakers; and process and governance approaches created inefficiencies and unnecessary rework.[24]

Defence now employs an approach that is more tailored to the level of risk and complexity associated with each project.[25] One important feature is the treatment of fundamental inputs to capability (FIC), with 'projects now scoped to be inclusive of all of FIC rather than materiel, infrastructure and/or IT-centric'.[26] Key elements include all major Defence capability and enabling projects use the *Smart Buyer* risk assessment framework to inform decisions about tailored approval pathways and project-execution strategies;[27] a shared understanding of risk throughout the capability lifecycle including with central agencies; establishing a single entity (the Capability Acquisition and Sustainment Group [CASG]) with governance and management responsibilities across the capability lifecycle; upskilling the workforce for the capability development, acquisition and sustainment functions through a centre-of-expertise model; and creating an environment of continuous improvement across Defence in support of the capability lifecycle.[28]

In addition to this, Defence recognised two other elements: that specialisation in capability design would be needed and that higher levels of government scrutiny should be expected. Defence has established two entities to perform the scrutiny function. The Force Design Division (within the Vice Chief of the Defence Force [VCDF] Group) is designed 'to test the force in being, provide preparedness assurance, design and guide the development of a balanced and affordable future force',[29] and the Contestability Division (within Defence) is designed to inform the 'development of the

---

[23] Australian Government, Department of Defence, 2012a.

[24] Australian Government, Department of Defence, 2015, p. 13.

[25] Australian Government, Department of Defence, *Capability Life Cycle Detailed Design: Executive Summary*, undated-a.

[26] Australian Government, Department of Defence, "The New Capability Life Cycle Has Commenced," *CASG Bulletin*, June 2016d.

[27] Australian Government, Department of Defence, "Smart Buyer," *CASG Bulletin*, June 2016e.

[28] As identified in Australian Government, Department of Defence, *Annual Report 16–17*, 2017a.

[29] Australian Government, Department of Defence, "Force Design Division," webpage, undated-b.

risk assessment and decision support framework to ensure that acquisitions are aligned with strategy and resources'.[30]

Reflecting on those areas that Defence have viewed as being most successful, Defence officials interviewed by the RAND team noted the importance of cultural change, as well as changes to process and procedures. They noted the importance of building a culture 'that allows a safe space for contesting and debating decisions'. This did not mean each committee representative 'champions a particular area'; rather, the sentiment holds that senior executives demonstrate 'intellectual honesty in interactions' and 'transparency' in decisions. The new model also matures the *capability manager* (CM) function, by empowering (and holds accountable) senior officials and military officers to establish capability requirements and then design, deliver and sustain capabilities that achieve these through their lifecycle within their area of responsibility.[31] Capability managers are resourced to undertake this capability management function, including retaining a capability-development role within their groups. Defence manages interoperability between capabilities through an Architecture Review Board; the Department currently has a similar construct.

Victoria Police Approach to Capability-Based Planning

In 2014, the Victoria Police institutionalised a capability-based planning (CBP) approach to capability development, in recognition that the force needed to adapt to major changes to its operating environment,[32] and that it lacked a strategy for achieving short-, medium- and long-term objectives in an efficient manner.[33] The Victoria Police approach was put forth in the *Victoria Police Blue Paper*,[34] which articulates the organisation's planned state over the 10-year period ending in 2025, and which spells out that the planned state will be achieved through 'better matching of resources to demand by rethinking the traditional operating model, and improving capability through workforce reform and technology; and collaborating more closely through

---

[30] Australian Government, Department of Defence, *2018–19 Defence Corporate Plan*, 2018, p. 6.

[31] A criticism of the previous model was that each of the service chiefs (the chief executive officers of the Defence Materiel Organisation and the Chief Capability Development Group) could and did change capability requirements over the lifespan of a project.

[32] Victoria Police, *Victoria Police Blue Paper: A Vision for Victoria Police in 2025*, State of Victoria, Australia, 2014, p. 7.

[33] State Government of Victoria State Services Authority, *Inquiry into the Command, Management and Functions of the Senior Structure of Victoria Police*, 2011.

[34] Victoria Police, 2014.

partnerships.'[35] The effort considers the full lifecycle of a capability and situates it within the strategic objectives of the organisation (see Appendix D).[36]

Taking a capability-centric approach, Victoria Police has established its own capability framework that integrates risk and uncertainty, capability and capability development, and resource management in a manner that provides informed and transparent decisionmaking.[37] Under the model, Victoria Police sought to use capability planning to understand where capabilities are in its lifecycle; design and choose between capabilities, particularly in response to new and emerging threats; understand the interdependency between capabilities; and establish a structured planning process that allows for effective investment prioritisation.[38] Further, Victoria Police employs a 'whole-of-life' approach to capability that ensures that investment extends beyond the initial capability development and acquisition phase and into sustainment and disposal. It has also recognised the resource implications for taking such an approach and has established an organisational entity with responsibility for managing their capability development function.

Victoria Police defines *capability* as 'what Victoria Police does, not where, why or how something is done', with characteristics that are 'representative of stable business functions, [that are] unique and independent from each other, [and are] independent of processes, organisation structure, and assets'.[39] Explicitly using the FIC construct to define how a capability is acquired and sustained, it identifies five FIC—processes, infrastructure, people, equipment, and technology—though it notes that the people component also includes training, capacity, knowledge and skills.[40] Victoria Police has identified 18 capabilities categories (with 78 subcategories), which it separates into eight core and ten enabling capabilities.[41] There is broad alignment between these capabilities and those required by the Department, particularly with respect to enabling capabilities.[42]

The initial step in Victoria Police's approach is the *capability plan*. This plan seeks to provide a roadmap for achieving the 2025 organisational vision established in the *Blue Paper* by articulating the key objectives, the service delivery functions, the

---

35 Victoria Police, 2014, p. 23.

36 Victoria Police, *Victoria Police Capability Plan 2016–2025: Capability Framework*, State of Victoria, Australia, September 2016.

37 Victoria Police, 2016, p. 4.

38 Victoria Police, 2016, p. 5.

39 Victoria Police, 2016, p. 10.

40 Victoria Police, 2016, p. 9.

41 Victoria Police, 2016, p. 17.

42 The RAND research team noted that the Victoria Police capability set is very large, and is likely to be difficult to manage, compare and optimise. RAND researchers anticipate that a smaller set of capabilities for the Department would be beneficial.

underpinning (core and enabling) capabilities and the FIC that contribute to these.[43] The capability plan is explicitly embedded within the internal planning process, and consists of the following five elements:[44]

- strategic and external drivers to situate the future operating environment
- capability framework to enable coordinated and planned actions to mature capabilities over the next decade
- maturity assessment to help prioritise capability development and inform investment decisions
- capability plan, which articulates the investments and organisational reforms required for capability development, delivery and sustainment
- annual plan, which outlines planned actions and activities to development, delivery and sustainment priority capabilities.

In discussions with Victoria Police, officials indicated the process commences with a six-month design (or 'sense-making') activity to define capability needs. Having described the capability, they then undertake a *capability impact assessment*, mapped against FIC, to establish an assessment of cost and benefit against their objectives. This requires the development of use cases for each capability option so as to assess their impact in a consistent manner. They then undertake a capability maturity assessment to assist in determining capability investment priorities, which includes assessing existing capabilities to determine if there is the need to disinvest. The output of this process is an investment pipeline that explicitly includes sustainment costs beyond the budgeting cycle. Victoria Police officials indicated that the threshold for seeking additional funding from government for capability projects is $10 million AUD.

Having completed the cycle, Victoria Police's assessment is that this approach makes it 'better [able to] assess and understand the maturity of all our organisational capabilities. It has also provided the focus to justify investments and reforms by demonstrating how each project contributes to building capability and the confidence of government and the community in our ability to manage our resources. Embedding the capability plan has realised benefits including:

- Establishing common language for business planning and decision-making.
- Facilitating greater alignment of plans and strategies across the whole organisation.
- Removing siloes and duplication of projects and processes.

[43] Victoria Police, 2016, p. 8.

[44] Victoria Police, 2016, p. 13.

- Facilitating common understanding of business direction and priorities across various levels of the organisation."[45]

Victoria Police emphasised in discussions with the RAND team that it was fundamentally important to get the construct for the CLMM correct before developing the underlying processes. Engaging effectively across the organisation was critically important. Interviewees indicated they have taken considerable time to engage and build relationships with their operator community to support the transition to their approach.

International Organisations

The Department has many similarities to peer organisations overseas, particularly the U.S. DHS and the UK Home Office (UKHO). In many cases, these entities have faced challenges in developing and implementing their own approaches to capability development. The RAND research team engaged with officials in or working with these organisations on capability development and acquisition functions. RAND researchers also engaged with the U.S. DoD in areas of particular relevance to the Department (e.g., rapid acquisition). This has enabled the research team to identify lessons and best practices for the Department, particularly from a portfolio perspective.

U.S. Department of Homeland Security

The U.S. DHS has a similar portfolio construct to Home Affairs and takes a similar capability-based approach to identifying, developing and employing systems of capabilities to meet government objectives. This report used the following two case studies to assess issues relevant to Home Affairs (see Appendix E):

- Joint Requirements Council (JRC): a centralised body which seeks to establish and harmonise capability requirements across portfolio agencies through a strategy-led approach
- Minotaur: a specific air domain mission-management system that represents an example of operator-driven capability development that works outside the standard acquisition approach.

Joint Requirements Council

The JRC provides the forum by which DHS seeks to identify cross-portfolio opportunities that enhance operational outcomes, effectiveness and efficiency across DHS. It seeks to validate and prioritise capability requirements for all major acquisitions through an objective and analytically rigorous approach.

[45] Victoria Police, 2016, p. 12.

The JRC has four macro-level mission areas. The first of these is the implementation and execution of Joint Requirements Integration and Management System (JRIMS), a process by which DHS reviews and validates capability gaps and determines capability requirements to mitigate them. The second is the provision of training to DHS staff on the requirements process, primarily focused on the JRIMS. The third responsibility is conducting analyses of joint capabilities and requirements, which incorporates assessing capabilities across DHS to create a prioritised list of gaps, and assessing existing programs to provide input to senior leaders on investment and funding decisions. The final mission is to engage in targeted outreach to various enterprise-wide forums related to requirements, as well as external engagements with entities outside of DHS.

The JRC comprises senior officials representing key DHS headquarters offices and seven of the department's operational components.[46] Through the JRC, these officials inform DHS investment decisions by representing the views of both their components and DHS, validating and prioritising capability needs and operational requirements, providing requirements-related advice, and validating key requirements documentation, supported by strong analytical rigor.[47] Recent U.S. Government Accountability Office (GAO)[48] reports have identified some lessons of particular relevance to Home Affairs, namely that the JRC

- must be a leadership priority if it is to be effective
- needs to understand the culture of its members
- should develop processes that break down barriers and remove organisational silos
- would benefit from having agile processes that are not onerous
- should avoid being too detailed in the capability-identification phase
- should reflect the DHS strategic and operating environment, and not simply transport the DoD model
- should establish requirements in a manner that can be tested and analysed.[49]

---

[46] The key offices are Customs and Border Protection, the Federal Emergency Management Agency, Immigration and Customs Enforcement, the U.S. Secret Service, the Transportation Security Administration the U.S. Coast Guard, and U.S. Citizenship and Immigration Services.

[47] U.S. Government Accountability Office, *DHS Acquisitions: Additional Practices Could Help Components Better Develop Operational Requirements,* report to Congressional Requesters, GAO-18-550, August 2018.

[48] The U.S. Government Accountability Office was known as the General Accounting Office until 2004, when its name was changed by an act of Congress. 'GAO' in this report refers to this body in both iterations.

[49] U.S. Government Accountability Office, *Homeland Security Acquisitions: Joint Requirements Council's Initial Approach Is Generally Sound and It Is Developing a Process to Inform Investment Priorities*, report to Congressional Requesters, Washington, D.C., GAO-17-171, October 2016.

Minotaur

Minotaur is a mission management system primarily used on surveillance aircraft by the U.S. DHS and DoD. It uses data from many sensors to create a common picture; automates some functions, such as moving sensors to focus on particular targets of interest; allows replay of sensor information; and tracks hundreds of potential targets at once.[50] That integrated information can be transmitted among aircraft and units in flight,[51] and to operations centres.[52]

Minotaur provides an example of a capability developed by one organisation being adopted and integrated by other organisations. It was originally developed by the U.S. Navy,[53] and is now being used or tested on several platforms, including three U.S. Coast Guard (USCG) surveillance aircraft,[54] four Customs and Border Protection manned and unmanned aircraft[55] and two U.S. Navy aircraft.[56] Minotaur is an open-architecture, government-owned system,[57] managed by the U.S. Navy and Customs and Border Protection's Air and Marine Operations (AMO) organisation since 2008.[58] The U.S. Navy, AMO and the USCG cooperate on modifications to Minotaur.[59]

Development and procurement of the Minotaur system intentionally took place outside of the standard DHS procurement system. In this nonstandard process, requirements for system enhancements are developed by the system operators and are implemented collaboratively by the user organisations.[60] System operators work side by side with the engineers developing the system, and there are no headquarters-level executive steering committees involved.[61]

The success of this project has been attributed to the close collaboration between system developers and operators. It was also noted that there was a cooperative approach to managing and developing Minotaur between the AMO, Navy and USCG. It is pos-

---

[50] Paul Koscak, "Innovative Tech Helps AMO Combat Smugglers," U.S. Department of Homeland Security, Customs and Border Protection, undated.

[51] U.S. Coast Guard, Acquisition Directorate, "Minotaur Mission System," fact sheet, April 2018.

[52] Mark Erwin, "Airborne Solutions for Maritime Border Security Operations: Minotaur Mission Management System," briefing delivered to U.S. Customs and Border Protection, August 2017.

[53] U.S. Coast Guard, "Minotaur Mission System," webpage, undated.

[54] The three aircraft are the HC-130J Super Hercules, HC-144 Ocean Sentry and C-27J Spartan.

[55] The four aircraft are the DHC-8, P-3 Orion, King Air 350 and the unmanned Predator.

[56] The two are the P-8 maritime patrol aircraft and the EP-3E electronic reconnaissance aircraft.

[57] U.S. Coast Guard, undated.

[58] Erwin, 2017.

[59] Discussion with DHS official, 29 August 2018, and Koscak, undated.

[60] U.S. Coast Guard, undated, and discussion with DHS official, August 29, 2018.

[61] Discussion with DHS official, 29 August 2018.

sible that the program would not have fared as well if there had been a less collaborative environment.[62]

U.S. Department of Defense

The U.S. DoD has extensive experience in capability development, albeit on a much larger scale than Home Affairs and within a significantly different political, operational and fiscal environment. While this can limit RAND researchers' ability to identify lessons, the project team identified the following two areas that provide useful insights (see Appendix E):

- the Joint Capability Integration and Development System (JCIDS) process to fill capability gaps
- the use of rapid acquisition processes to field operational capabilities.

Joint Capability Integration and Development System

The JCIDS process aims to identify, assess, validate and prioritise the capabilities required to fulfil the DoD's missions.[63] Upon identification of a capability gap, it seeks to resolve capability shortfalls by exploring combinations of materiel and nonmateriel solutions (see Appendix C). Early in the process, an analysis of alternatives (AoA) is performed. The AoA compares the effectiveness and cost of different alternative solutions that could fill a capability gap and enables decisionmakers to select a preferred capability option. Three components are key to any AoA: context to situate capability needs, alternatives for addressing those needs, and a range of different analyses to explore the full complexity of the operational and strategic environment. When combined, these lead to trade-off analyses, which compare costs, effectiveness and risks across all alternatives.

Rapid Acquisition

The DoD also uses alternative rapid acquisition approaches in some circumstances. For this project, the RAND team explored two rapid acquisition programs:

- Predator: an unmanned aerial vehicle (UAV) that provides real-time intelligence, surveillance, and reconnaissance (ISR) and strike capabilities to tactical commanders. It was acquired using a rapid acquisition approach designed to insert

[62] Discussion with DHS official, 29 August 2018.

[63] Defense Acquisition University, "Program Management," *Defense Acquisition Guidebook*, U.S. Department of Defense, undated-a, section 1-3.2.

commercially developed technologies into the defence acquisition process in mid-stride.[64]
- Palantir Intelligence Analysis Software: an intelligence analytics environment employing proprietary software that was adapted to suit DoD needs. Licences for its use were bought through a rapid acquisition approach.

These programs demonstrate that while rapid acquisition and innovation approaches can work well to meet short-term needs, they can create legacy issues for the operating organisation, particularly if there is a need to expand production of a system, to extend its use more broadly across an organisation, or to integrate it into a broader operational context. Further organisational challenges can include intellectual property (IP) and proprietary property concerns, along with training, logistics, sustainment and integration issues. That being said, these programs provide the following insights into designing capabilities using the following rapid acquisition approaches:

- broad design guidance is best for rapidly developing new technologies
- focusing on a limited number of priority goals helps maintain speed during rapid acquisition
- engaging a broad range of stakeholders can help to build confidence and minimise bureaucratic resistance to rapid acquisition projects
- using multiple, flexible approaches and engaging multiple stakeholders gives rapid acquisition projects the best chance to be supported
- rapid acquisition projects can benefit from an iterative approach
- medium-term planning is still required to address eventual issues and shortcomings.

UK Government

In establishing the Home Affairs Portfolio, the Australian government was strongly influenced by the experiences of the United Kingdom, in particular the UKHO.[65] Therefore, the RAND team undertook three case studies that explored the UK system, namely,

- a risk-based cross-government capability-mapping approach to resilience in the context of civil emergencies

---

[64] This was known as the Advanced Concepts Technology Demonstrator (ACTD) program. See Michael R. Thirtle, Robert V. Johnson, and John L. Birkler, *The Predator ACTD: A Case Study for Transition Planning to the Formal Acquisition Process*, Santa Monica, Calif.: RAND Corporation, MR-899-OSD .

[65] Parliament of Australia, *Legal and Constitutional Affairs Legislation Committee: Estimates, Department of Home Affairs*, 26 February 2018.

- a new strategic planning operating model being established within the UKHO to support capability development
- a new approach to research and development for UKHO that integrates its science and technology (S&T) function with the UK Ministry of Defence (MoD) and manages this through a commissioning hub.

Cross-Government Capability Mapping

The UK government is putting in place a rigorous analytical approach to establish a capability map that provides a range of policy insights and supports cross-department actions as part of the Resilience Capabilities Programme (RCP) (see Appendix E.3). The RCP is being created in response to the belief that government departments were assessing and developing capabilities in silos, independently of each other, and that they lacked a common framework against which capabilities could be assessed.[66]

The UK government recently undertook a multiagency capability-mapping exercise based upon SME self-assessment from across government and against the UK National Risk Assessment.[67] The assessment framework prompts SMEs to rate a capability, assess the evidence on which they base their rating, and assess the criticality of the capability. From this, the relative readiness to respond to the identified risks can be assessed for each capability.[68] The result is a single visualisation aggregating this information.

This case study represents an example of capability mapping that aligns with the Department and ABF's aspiration to a risk-based, strategy-led portfolio view of capability. Some lessons identified include:

- ensuring common framework with definitions of capabilities and FIC
- employing a transparent, evidence-based and systematic approach to arrive at the assessment
- assessing the robustness of evidence base underlying the mapping—this is a crucial part of the model as it allows users to distinguish low-rated capabilities from instances in which information about the capability is missing
- visualising the products effectively to make them more user-friendly, so that the overall picture of capability can be easily understood
- championing the value of the exercise itself and stressing the efficiency savings for government departments if they engage in the approach.

---

66 United Kingdom Government, Cabinet Office, "Resilience Capabilities Programme Sunburst Policy Insights (Annex 2)," unpublished presentation, 2018c.

67 Organisation for Economic Co-operation and Development, "The UK's National Risk Assessment (NRA)," website, undated.

68 United Kingdom Government, Cabinet Office, "Resilience Capabilities Programme Understanding Capability (Annex 5)," unpublished presentation, 2018e.

Strategic Planning Operating Model

Like the Home Affairs Portfolio, the UKHO is seeking to overcome the limitations in its capability development approach. These limitations include a lack of common definition of capabilities, no comprehensive picture of capabilities nor why they need to reside within the UKHO, differing frameworks and approaches to capability planning across agencies, the tendency for near-term thinking, inconsistency between vision and objectives across entities, a tendency for bottom-up planning, and institutional barriers between agencies.

UKHO's response to these shortcomings is to develop a new strategic planning framework (SPF) (see Appendix E.3). This ongoing effort takes a means-ends approach and projects it on a ten-year outlook and a five-year planning horizon. Layered upon this approach are 'influencers,' namely lines of development (i.e., FIC) and analysis.

In moving toward a capabilities approach, the UKHO has confronted some issues that are similar to those identified in Australia. These include, for example, having the appropriate organisational structure required to design, acquire and operate capabilities most effectively, and determining whether these capabilities are best situated within UKHO.

Because the SPF is still in development and not yet embedded in the work of the UKHO, we must take care drawing insights. With this in mind, some initial lessons from SPF process include the following:

- invest in engagements with key representatives to achieve a consensus on SPF and the framework
- hold early consultations with stakeholders in bodies and agencies within the UKHO that have some independence in the way they operate
- establish and remain consistent with the core principles of planning and capability mapping
- build a common capability lexicon to address the issue of different agencies using different language to describe common capabilities
- focus on capabilities, not activities, and overcome the tendency to describe activities as capabilities
- develop the strategic vision and objectives that are SMART (specific, measurable, achievable, relevant or results-oriented, time-bound), but recognise that these can take time to mature
- recognise that organisational culture can inhibit change, and respond by establishing mechanisms that incentivise change and motivate participation.

Centre for Applied Science and Technology Commissioning Hub

The UKHO has a discrete entity to provide S&T support, the Centre for Applied Science and Technology (CAST). Over the last two years, work has started to establish

a Commissioning Hub within CAST to coordinate the identification of research and development needs across the whole of the UKHO,[69] which is overseen by a UKHO Science and Technology Oversight Board. (See Appendix E.3 for more details.)

Through the Commissioning Hub, the UKHO now has a consistent approach to identify S&T capability needs (in a similar manner to the approach taken by the UK MoD). The aim is for a shared framework which allows for common needs to be identified, efficiencies to be enabled, and shared learning to occur. The Hub has a mandate to commission scientific and technological research and innovation to address these needs, although this had not yet happened at the time this report was written (October 2018).

The vision behind the Hub is a shared-services model that transcends department and portfolio boundaries. Clearly, the opportunity for a key enabling function (in S&T) to leverage benefit from larger and more-established program represents an example of how the Department and ABF might seek to support capability development in a functional area where it has narrow areas of deep expertise. That being the case, lessons that have emerged so far from the United Kingdom's experience through the early stages of the Hub include the following:

- securing senior-level buy-in, both to the idea of the Hub and to the principle of a common approach, and establishing an oversight board
- taking time, once senior support is confirmed, to explain the new approach to all components of the organisation
- creating a dedicated team with the mandate to determine if, how and where research and development can support capability needs
- leveraging instances where a common approach has brought benefits to further secure buy-in
- taking a longer-term focus for developing capability and commissioning research to address future needs.

Summary of Observations

Bringing together the information from the sections above, this section examines the evidence base and makes 12 overarching observations that are used as the basis of the capability development framework for the Department and ABF in the following chapters. These findings are shown in Table 2.2 (see Appendix F for more details) and form the basis of the proposed framework, principles, models and internal capabilities presented in the remainder of the report. It should be noted that the RAND team was

[69] United Kingdom Government, Home Office Science Advisory Council, "Minute of the Home Office Science Advisory Council," 28 September 2017.

unable to interview senior officers from AFP, ASIO, ACIC and AUSTRAC. While this represents a limitation, the team believes that the consistency in responses between the Portfolio and other peer organisations is suggestive that these findings may be broadly applicable across the Portfolio. However, this conjecture should be confirmed by engagement with Portfolio agencies during implementation.

Table 2.2
Key Observations for Enhancing Capability Development Within Home Affairs

Observations	Explanation
Organisational patience: Institutionalising a capability lifecycle approach across the Portfolio will take time, resources and commitment from senior management, as it entails changes to governance, organisational culture, processes, and training and development.	Although senior management appreciates that a properly constructed capability lifecycle approach across the Department and ABF (and, possibly, the Portfolio) will take time, resources and commitment to initiate and institutionalise a more mature approach and the extent of the required resources and commitment is not well understood.
Internal appetite for change: There is an appetite among the senior Departmental and ABF staff to change to a strategy-centred approach for capability development and acquisition that incorporates a whole-of-life perspective, rather than focus on the acquisition and operations phases.	Notwithstanding the above, there is an appetite for change among senior Department and ABF staff to move to a CLMM that is demonstrably strategy-led and fully encompasses the full cycle through development, acquisition and sustainment through to disposal.
Risk versus threat as the frame of reference: There is a tension between those who favour pursuing a threat-based approach to capability development that focuses on specific threats which tend to lead to investment in solutions to address immediate short-term issues, and those favouring a risk-based approach treatment that seeks to design capabilities to that meet enduring challenges.	While acknowledging that a strategy-led approach is needed, there is disagreement among the senior staff as to whether the strategy should be based on specific threats or against a broader risk-based assessment of the environment.
Not a unique journey: All peer organisations are addressing this issue, with the UKHO and Home Affairs on a similar trajectory in developing and implementing a capability framework. The United Kingdom is slightly more advanced.	Six peer organisations were explored, and all were seeking to establish some of a structure capability development lifecycle. All had similar definitions of capability, employed a FIC-like model and identified the need for enabling capabilities. We observed that there is a particularly close alignment between the UKHO and Home Affairs, as are both developing reformed capability development policies and procedures along similar lines. However, the UKHO program is more advanced. We believe that the Department should monitor the progress of the UKHO in order to take note of 'lessons observed'.

Observations	Explanation
Building trust through transparency: Home Affairs needs to develop and employ a robust and transparent process that incorporates all elements of the capability lifecycle in order to give government the confidence it needs for capability investment approvals.	Our interviews with the central agencies and Defence show that Home Affairs needs to employ, and be seen to employ, a robust process that is transparent throughout the CLMM if it is to be successful in gaining government approval for significant investments.
Tailored governance: Governance structures tailored to the complexity, size and risk of each program are required in order to give capability development programs greater agility and assurance.	Experience in both Australia and overseas in CLMM is that CLMM governance structures need to be tailored according to the complexity, size (cost) and, most importantly, risk, associated with a specific capability development. We saw no evidence of this in the Department.
Collaborative culture: There is a need for a more collaborative and collegial culture between policy, acquisition and operational staff, at all levels, as an essential prerequisite for establishing a resilient capability lifecycle management model.	Culture is important. We observed a clash of cultures between the Policy, Acquisition and Operational staffs of the Department and the ABF that needs to be addressed if a robust and resilient CLMM is to operate efficiently and effectively. A consistent approach to capability development with clear role delineation can assist with that.
Strategy-led: Robust capability development requirements need to be clearly linked to capturing operational needs and traceable to strategic objectives.	We did not see a clear process for requirements capture. We did not observe any Department policies or processes that gathered operational needs in a structured and consistent manner, nor a system that linked them to strategic objectives in a coherent and traceable way. We also see a strong need for the Department to establish clear strategies and guidelines to engage early and frequently with key stakeholders, especially the central agencies, to instil confidence in their process.
Phased rollout: A phased rollout for the implementation of the agreed approach is necessary to ensure that the Department can build internal competencies in capability development and project management.	The literature shows that the 'big bang' approach to reforming the capability development process in Department of the size and complexity of Home Affairs will not work. A phased approach is needed in order to give time for the systems and associated competencies to be brought up to speed.
Consistency improves quality: The quality of capability decisionmaking is currently constrained by Home Affairs' lack of maturity and consistency in policies, frameworks and language.	There is general agreement among senior Department and ABF staff that the quality of capability decisionmaking is limited, owing to a lack of maturity and consistency in policies, frameworks and language across the various constituent parts. Undertaking analysis to build the evidence base is a recognised need.

Observations	Explanation
Forward-looking: Local and international experiences demonstrate that robust research, development and innovation (RD&I) programs are essential for future-proofing Home Affairs by enabling the exploration, acquisition and integration of new capabilities within dynamic environments.	There is ample evidence both in Australia and overseas that in a government department (or portfolio) that relies ever increasingly on advanced technology that a significant investment in RD&I in general pays dividends. We believe that the current Department RD&I program is not designed to future-proof the organisation as it does not look far enough into the future, and there is inadequate investment.
Dedicated internal capability: Implementing a sustainable CLMM successfully requires an appropriate organisational structure with capacity built around the competencies of permanent staff.	It is axiomatic that a robust, resilient, streamlined and efficient CLMM requires the appropriate quantum of properly skilled personnel. Experience in Australia and overseas shows that this is best served through a dedicated and accountable organisational entity with a permanent cadre of staff and supported by a functional knowledge management system. This is currently lacking in the Department, with the Capability Planning and Development Branch being used to fill the void, which lacks sufficient staff to do this in addition to their other responsibilities. It is difficult to envisage the successful implementation of the CLMM if this is not addressed.

CHAPTER THREE

A Capability Development Framework for Home Affairs

This chapter proposes an overarching CLMM framework for Home Affairs. It is built upon a set of design principles tailored for capability development practice within the Department and ABF. It defines capability and recommends an update to the current FIC model employed within the Department and ABF It concludes by identifying the enabling functions necessary to support capability development within the Department.

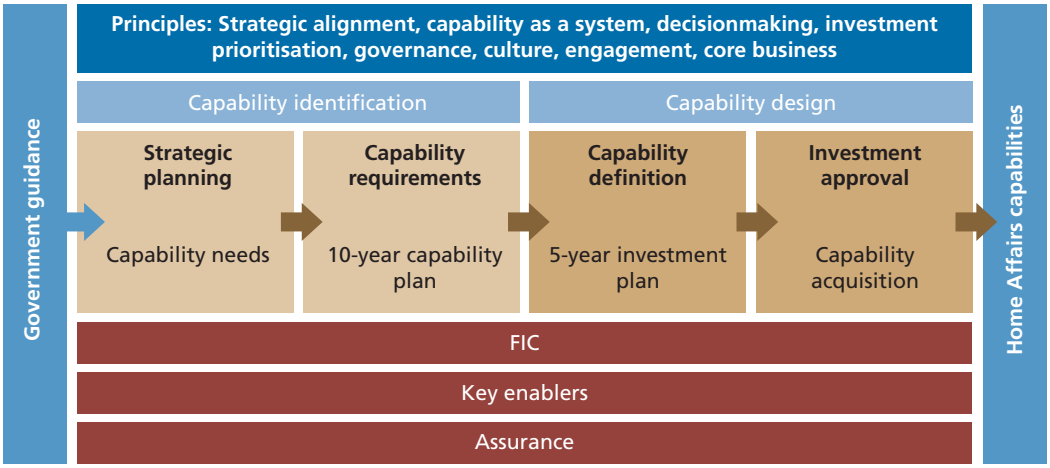
Overarching Framework

To assist in understanding the overarching logic of the capability development lifecycle, the RAND team established an overarching framework (see Figure 3.1). This framework captures the essential activity of capability development, namely the translation of government guidance into the delivery of effects and outcomes in a cost-effective and sustainable manner. Within the framework, capability development can be aggregated into the following two major activities:

- **Capability identification:** takes strategic guidance, translates it into operational tasks and then capability needs. Prioritised gaps are identified and capability options are explored to establish a 10-year capability plan. This represents phases 1 (strategic planning) and 2 (capability requirements) of the CLMM depicted in Figure 3.1.
- **Capability design:** develops the acquisition strategy for capability development by establishing the medium-term investment program from which individual capability projects establish their business cases for approval. This represents phases 3 (capability definition) and 4 (investment approval) of the CLMM depicted in Figure 3.1.

Figure 3.1 also displays the broader elements that support and enable those activities. The principles that underpin capability development, the individual elements that

Figure 3.1
Capability Development Framework



contribute to a capability, the enabling functions that the system requires, and the ability to ensure scrutiny must be applied throughout the phases of the CLMM.

Principles for Capability Development

In exploring capability lifecycle management best practices, the RAND team elected to use the current Defence approach as the basis for developing a more-mature CLMM. While it is clear there are some fundamental differences between the Home Affairs Portfolio and the Defence Portfolio (as discussed in Chapter Two), the authors note that each department must operate in, and be compliant with, the same overarching decision environment. Both must comply with the Public Governance, Performance and Accountability Act (PGPA)[1] and have department ministers who are members of the National Security Committee of the Cabinet. Further, a significant number of senior Home Affairs officials have previously worked in Defence, and have demonstrated knowledge of Defence's approach to capability lifecycle management (see Appendix D.1).

Drawing upon the baseline review of the way in which the Department and ABF currently undertake capability lifecycle management (see Appendix F), and of lessons from international CLMMs (outlined in Chapter Two), the project team identified the

[1] Australian Government, Department of Finance, *Public Governance, Performance and Accountability Act 2013*, 2013.

following eight principles that capture the key characteristics for designing and applying a mature CLMM:

1. **Strategic alignment:** Capabilities should be defined in terms of effects or outcomes that are traceable to strategic objectives, operational tasks and organisational functions.
2. **Capability as a system:** A capability is a system of interlocking and interdependent elements that, when combined, deliver one or more outcomes or effects. Capabilities should be grouped and partitioned into constructs that reflect department and agency missions that help enable effective program management.
3. **Decisionmaking:** Capability development decisions should be evidence-based, risk-informed, designed to accommodate emerging threats and opportunities, and incorporate interdependency implications. In order to achieve this, staff need to be appropriately skilled,[2] empowered[3] and positioned within the organisation.[4]
4. **Investment prioritisation:** Capability investment should consider the entirety of the capability lifecycle, be prioritised in accordance with a strong evidence base, and be internally contested at levels appropriate for its size, risk and complexity.
5. **Governance:** Capability development decisions should be made with accountability, transparency, integrity, stewardship, efficiency, effectiveness, leadership, teamwork and sustainability.[5] Decisions should be made with the involvement of a senior executive, a condition that demonstrates unity of purpose, an ownership of the decisions made, an understanding of the importance of taking appropriate risks, and a willingness to divest from capabilities as circumstances dictate. Timelines, key decision points, resources and interdependencies should be monitored throughout the capability lifecycle to ensure the capability development process is being managed effectively.
6. **Culture:** The organisation should embrace a collaborative culture that values intellectual honesty and transparency, encourages contesting and debating ideas when making decisions, accepts those decisions once they are made, and places the good of the enterprise over championing one's own organisational domain.

---

2 See Chapter Six for more detail.

3 'Empowered' means ensuring that staff are directly involved in the planning process to develop requirements from a frontline perspective.

4 Appropriate organisational alignment has been found to be a key contributor to the success of capability development functions within government organisations.

5 See Appendix J for details on each of these terms.

7. **Engagement:** Capability development decisions should be made in close consultation with relevant SMEs and may benefit from close engagement with such experts as an integral part of the development process. Close consultation with all relevant Commonwealth, state and territory agencies and international partners is a crucial component for the planning, development and utilisation of Home Affairs capabilities.
8. **Core business:** Home Affairs should seek to develop and deliver only those capabilities that cannot be delivered more effectively and efficiently by other entities.

Combined with the 12 findings outlined in Chapter Two, these eight design principles reflect opportunities, challenges and guidelines for the Department and ABF to design, deliver and sustain capabilities. Central to this is the development of a robust, transparent, scalable and repeatable approach that improves internal capacity to build, operate and sustain capability throughout its life. Should such an approach be taken, the Department will be able to demonstrate the benefit of government investments through clear linkages to government priorities and Portfolio outcomes.

Capability and Its Fundamental Inputs

Principles one and two capture the essence of what constitutes capability, with the former establishing its conceptual basis in effect or outcome (see right-hand side of Figure 3.1), while the latter captures its construct through the integration of materiel and nonmateriel elements. Capability, as currently used within the Department and ABF, 'is defined as the capacity and intent to achieve and sustain a desired effect or output in order to meet one of more strategic objectives'.[6] Having reviewed definitions in similar organisations,[7] the RAND team believes this current definition is sufficient to meet Home Affairs needs.

DIBP had previously developed its own FIC and associated definitions, which have been taken as the initial set of FIC for the Department and ABF.[8] To assess their adequacy, the study team compared those definitions to other FIC-like models in Australia, the United States and the United Kingdom (see Appendix C). The set used

---

[6] Australian Government, Department of Home Affairs, 2018f, p. 2.

[7] See, for instance, Australian Government, Department of Defence, 2012a, p. 2; Australian Federal Police, *Policing for a Safer Australia: Strategy for Future Capability*, March 2017, p. 30; Yi Yue and Michael Henshaw, "An Holistic View of UK Military Capability Development," *Defense & Security Analysis,* Vol. 25, No. 1, March 2009, pp. 53–67.

[8] We were unable to find an endorsed document with FIC definitions. These definitions came from Australian Government, Department of Immigration and Border Protection, *Capability Management*, unpublished presentation, 2017b.

by the Department appears consistent with comparable FIC-like models, though the Department has identified the need for an 'industry' FIC. The RAND team could find no explicit definition and therefore developed a definition based on the one employed by Defence.[9]

The analysis showed that the Department does not have a FIC dedicated specifically to capture 'organisation' (which currently is captured loosely under 'support'). Given the more complex organisational structure associated with the Portfolio; and the intent to focus effort and avoid duplication, work across portfolio agencies, and seek efficiencies, there is a clear need to incorporate a FIC element that considers organisation explicitly. Otherwise, there is a risk that capabilities could be stovepiped into functional areas, which was a concern raised by many interviewees. The study team recommends an organisation FIC that incorporates the structural elements within the Department and the Portfolio agencies; the distribution of the workforce across each of these functional areas; and the overarching leadership, control and governance mechanisms that enable coordination across these areas.

Noting the above, and based on our review of international practices and discussion with senior officials, the RAND team recommends that Home Affairs use the following set of FIC and associated definitions:

- **People:** the appropriately sized workforce that has the necessary skills to perform the required role.
- **Training:** the education and skills development programs which enable the workforce to acquire and maintain appropriate skills and competencies.
- **Facilities:**[10] the supply, development, and maintenance of infrastructure required to effectively implement specific capabilities.
- **Information and systems:**[11] the reference and support materiel essential for the delivery of capabilities.
- **Equipment and supplies:** the assets, hardware and materiel required to implement capabilities.
- **Support:** the operational and corporate services that underpin capabilities, such as finance and maintenance support.
- **Laws, policies, procedures and administration**: ensuring that a capability incorporates all levels of required documentation and guidance.

---

[9] Australian Government, Department of Defence, *Defence Industry Policy Statement*, 2016b, p. 19.

[10] We note the emphasis on the support to the specific capability. As such, the broader critical infrastructure needs are considered separately as a key enabler.

[11] As is the case for Defence, information and communications technology (ICT) is an important and strategic asset for the Home Affairs Portfolio (see Australian Government, Department of Defence, 2016a, p. 84). Because of this, we treat it as a key enabler.

- **Industry:** the capabilities of Australian industry and the capacity of Australian businesses to deliver not only operational and other capabilities, but the full spectrum of support functions.
- **Organisation:** the appropriate structures, personnel and balance of competencies to accomplish operational tasks and to ensure appropriate leadership, control and coordination.

Key Enablers

Key enablers are enterprise-level functions that support and contribute to the efficiency, effectiveness and sustainment of operational functions.[12] They differ from FIC elements because key enablers are crosscutting and concurrently contribute to a number of functions and capabilities. Each enabler should be treated as a strategic asset with its own enterprise-level plan and investment strategy that most effectively and efficiently invests the Department's finite resources into the right capabilities at the right time.[13] These would be key components of the Department and Portfolio strategies. Because of this, these enablers need to be incorporated into the capability plan and integrated investment program to ensure that they are properly accounted for when determining the resources required to achieve the ambitions of the Portfolio, particularly as Home Affairs is seeking to enact a shared-services model that centralises such enabling capabilities.

We note that, within the Australian context, key enablers are recognised and considered within the capability lifecycle. For instance, Defence identified 14 enabling capabilities in its 2012 *Simplified Business Model*;[14] in its 2016 *One Defence Business Model*, Defence identified six enablers, four "direction setting and contestability" functions and four controls.[15] Similarly, Victoria Police have identified ten enabling capabilities.[16] For a comparison, see Appendix C.2.

Unlike FIC, key enablers tend to be more dependent on the particular operational environment. As such, a simple translation is not possible. Using the analysis in Appendix C.2, and incorporating issues raised in our discussions with Home Affairs senior management, the RAND team suggests that key enablers for Home Affairs should include the following:

---

[12] It is important to note that key enablers and operational capabilities should be considered on equal footing.

[13] Australian Government, Department of Immigration and Border Protection, 2016, p. 2.

[14] Australian Government, Department of Defence, *The Simplified Defence Business Model*, undated-c, p. 3.

[15] Australian Government, Department of Defence, 2016a, p. 168.

[16] Victoria Police, 2016, p. 17.

- **Capability development:** the function by which Home Affairs establishes, analyses and promotes its case for capability investment from government.
- **ICT:** the enterprise-level architecture and systems that underpin all Home Affairs capabilities.
- **RD&I:** the overarching strategy that future-proofs the organisation, capitalises on new opportunities and mitigates emerging threats.
- **HR:** the strategic personnel plan that delivers the quantity and quality of people necessary to meet organisational demands while adhering to corporate and legal responsibilities.
- **Strategic budgeting:** the capacity to develop budget forecasts that inform enterprise-level planning across all relevant time frames.
- **Critical infrastructure and estate management:** the estates and physical infrastructure necessary to support the delivery of all functions across the enterprise.
- **State and territory engagement:** the provision of national-level coordination across key Home Affairs domains through strategic and operational relationships with domestic partners.
- **International partnerships:** strategic collaborative arrangements with international peers to enhance the capabilities of Home Affairs and its regional partners, and to be a conduit for domestic partners.

Assurance and Contestability

As discussed earlier in this chapter, the overarching policy for ensuring good governance by Commonwealth entities is the PGPA.[17] The objectives of the PGPA include establishing 'a coherent system of governance and accountability … [and] a performance framework across Commonwealth entities' thus ensuring Commonwealth entities 'meet high standards of governance, performance and accountability'.[18] Application of the PGPA is standard practice across the Portfolio, and provides external assurance by informing both government and the Australian public on the Portfolio's performance. From a capability development perspective, it offers standardised responsibilities and duties, institutes a measurable performance-based approach that specifically focuses on outcomes and objectives, and instils a risk-informed approach to improve performance and decisionmaking.[19]

---

[17] Australian Government, Department of Finance, *Resource Management Guide No. 130: Overview of the Enhanced Commonwealth Performance Framework*, 2016b, p. 3.

[18] Australian Government, Department of Finance, 2019.

[19] Australian Government, Department of Finance, *Commonwealth Procurement Rules: Achieving Value for Money*, 1 January 2018.

While the PGPA provides the basis for external assurance and scrutiny, it assumes these functions are built upon existing internal processes. From a capability development perspective, the application of a governance model and the practice of contestability offer mechanisms for internal assurance that can improve the quality of capabilities allow more efficient expenditure of resources, build resilience through understanding a mature approach to risk, and act as a confidence-building measure with government and external agencies.[20]

The contestability function examines key elements of a project (e.g., alignment to strategic objectives and cost) and has a role in project oversight from the capability requirements stage through to divestment. The fundamental purpose of contestability is to ensure that Home Affairs makes robust and informed investment decisions.[21] The expectation for contestability within the public sector (i.e., beyond the contestability function that resides within Defence) can be seen by the recent Australian National Audit Office (ANAO) report that found a structured program for contestability 'was effective in supporting entities to review the efficient and effective delivery of government functions'.[22] Given that incorporating a contestability function into Home Affairs will have resource implications, developing an appropriately tailored contestability framework will be necessary.[23]

---

[20] Governance is discussed in more detail in Chapter Five.

[21] Adapted from Australian Government, Department of Defence, *The CASG Business Framework*, 2017b, p. 3.

[22] ANAO, "Efficiency Through Contestability Programme," webpage, 20 May 2018a.

[23] For a review of international practices in contestability, see Cynthia R. Cook, Emma Westerman, Megan McKernan, Badreddine Ahtchi, Gordon T. Lee, Jenny Oberholtzer, Douglas Shontz, and Jerry Sollinger, *Contestability Frameworks: An International Horizon Scan*, Santa Monica, Calif.: RAND Corporation, RR-1372-AUS, 2016.

CHAPTER FOUR

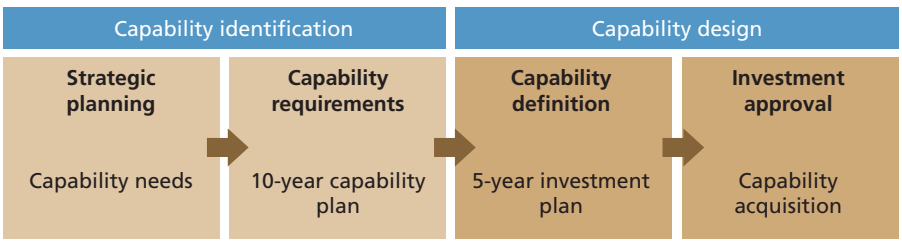
Capability Development Logic Models from Strategy to Investment Decisions

Having established the components that underpin the capability development framework (Figure 3.1), this chapter will employ a CBP approach to establish the logic models and underlying processes for the capability development phases of the CLMM (namely, the first four phases of Figure 2.1). These phases are shown in the orange boxes in Figure 4.1.

As noted in Chapter Three, the framework separates the phases focusing on identification of the capability (culminating in a 10-year capability plan) from those focusing on the design of the capability solution (which establishes a medium-term investment program that then leads to investment approval). A brief overview will be given for the capability identification and capability design phases, with a simple and a mature logic model presented for each phase. The mature model represents best practices, while the simple portrayal provides an interim model that could be employed by the Department as it moves toward the mature model. It should be noted that greater detail for each of these phases is provided in Appendixes G and H.

Readers should also note that, when taken together, these phases form the basis of an annual planning cycle, and thus this chapter provides an outline for that action. However, the detailed planning cycle will need to be developed during the imple-

Figure 4.1
Capability Development Phases of CLMM



mentation of the model, once the Department confirms the process models and governance approach.

A Capability-Based Planning Approach

CBP has been defined as 'planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances, while working within an economic framework'.[1] Best practices in CBP seek to deliver 'an effective investment strategy that develops and sustains the capability priorities identified through the planning exercise. These capability development directions can then be used to prepare a Capability Development Plan supported by an Integrated Investment Plan. A systemic approach will ensure both an audit trail and a logical performance management framework'.[2]

The proposed capability lifecycle model for the Department is depicted in Figure 4.1.[3] This figure shows that a CBP approach has been employed for the first four phases of the CLMM. CBP approaches have been used extensively in organisations such as the Departments or Ministries of Defence in Australia, Canada, the United States and the United Kingdom;[4] the Victoria Police;[5] and the U.S. DHS.[6] Such an approach to the capability lifecycle implies that the underlying focus is on managing risk over time and across the operating environment, rather than seeking to adjust systems to address specific threats. The employment of a CBP approach is essential to ensure the Department to takes a long-term, strategy-led approach.[7]

Finally, it is important to understand the universal standard for a capability lifecycle. We note that the International Standard for Asset Management suggests that assets need to be supervised within a system that recognises that grouped assets are best managed in a portfolio construct that coordinates the relationships and interdependencies between assets, while recognising that each asset has its own lifecycle. [8]

---

1 Paul K. Davis, *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation*, Santa Monica, Calif.: RAND Corporation, MR-1513-OSD, 2002, p. 1.

2 Technical Cooperation Program, "Guide to Capability-Based Planning," 2004, p. 3.

3 See Australian Government, Department of Home Affairs, 2018f.

4 Stephan De Spiegeleire, "Ten Trends in Capability Planning for Defence and Security," *RUSI Journal*, Vol. 156, No. 5, 2011, pp. 20–28.

5 Victoria Police, 2016.

6 Sharon Caudle, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community," *Homeland Security Affairs*, Vol. 1, No. 2, August 2005.

7 Australian Government, Department of Home Affairs, *A Strategy-Led Approach to Portfolio Capability Investment: Draft,* internal document, 2018c.

8 International Organization for Standardization, 2014.

The ISO55000:2014 standard breaks down the asset lifecycle into four distinct phases: planning, acquisition, operations and sustainment, and disposal. The capability lifecycle approaches that the research team reviewed (including the framework used within the Department) are consistent with the international standard.

Definitions

Analysis of the definitions provided in the Capability Review Terms of Reference, discussions with senior staff, domestic and international practice, and reviews of relevant policy documentation suggest that the current definitions that are used for each of the first four phases of the CLMM require revision. In accordance with international best practices, the RAND team recommends using the following definitions:

- **Strategic planning** focuses on strategy and its role in informing and shaping capability development. It provides a risk-based view of the Department's present and future direction to inform forward planning of investment across the life of a capability, including acquisition, operations, sustainment and disposal.
- **Capability requirements** is the point at which high-level capability gaps are identified, prioritised and endorsed. Capability proposals (incorporating capability needs statements and indicative budget provisions) are developed, and likely funding mechanisms identified, either externally via funding instruments such as a New Policy Proposal (NPP), or internally through the Departmental Capital Budget (DCB).
- **Capability definition** encompasses the establishment of capability proposals, the development and exploration of options for addressing the capability requirements, and the development of business cases to support prioritisation across a multiyear integrated investment program.
- **Investment approval** transforms prioritised capability options into well-defined and costed solutions incorporating all FIC, which include whole-of-life workforce numbers and budgetary provisions to acquire, operate and sustain the capability solution.

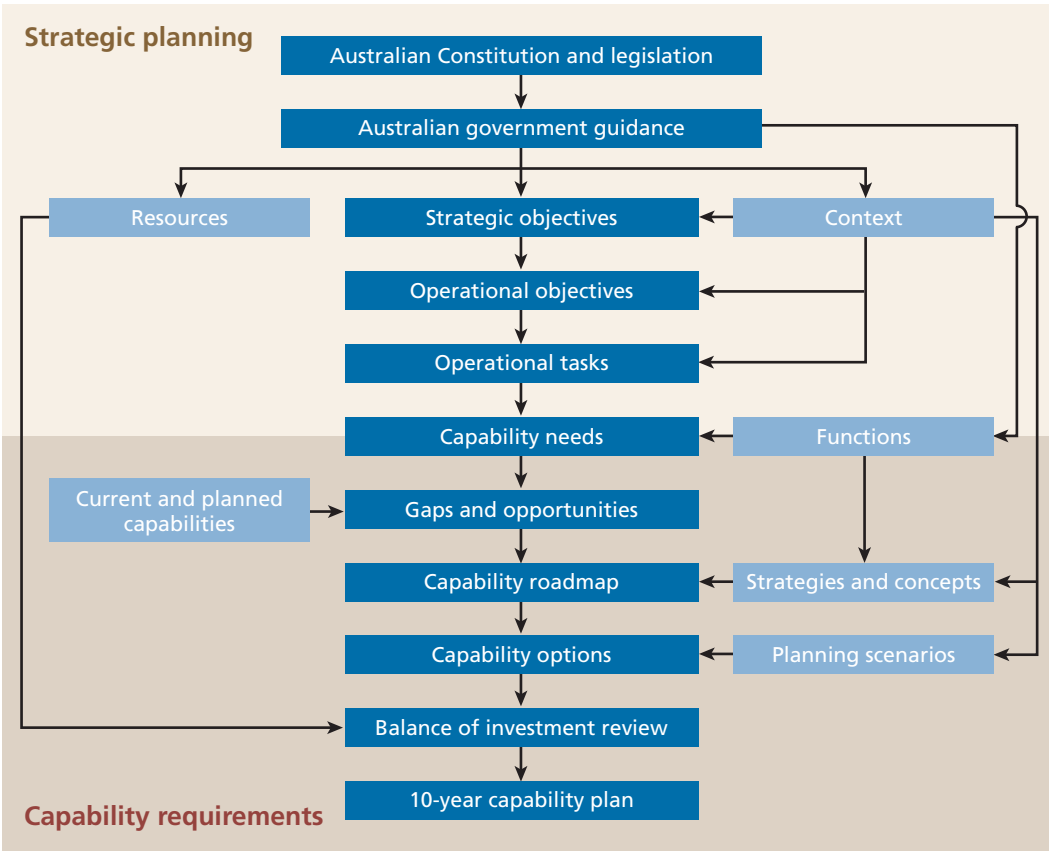
Capability Identification Activity

Capability identification is the key function of the first two phases of the CLMM. Through this process, the underlying logic linking government guidance and the long-term plan for delivering capability is established. Government support to the process is critical, since the CLMM will convey to the government the level of national security risks they are accepting, given the resources that are being provided, while providing

surety to the Department when developing the individual capability project. From a more pragmatic perspective, the research team believes that capability identification and capability design each represent constructs around which the Department can organisationally structure itself (see Chapter Six).

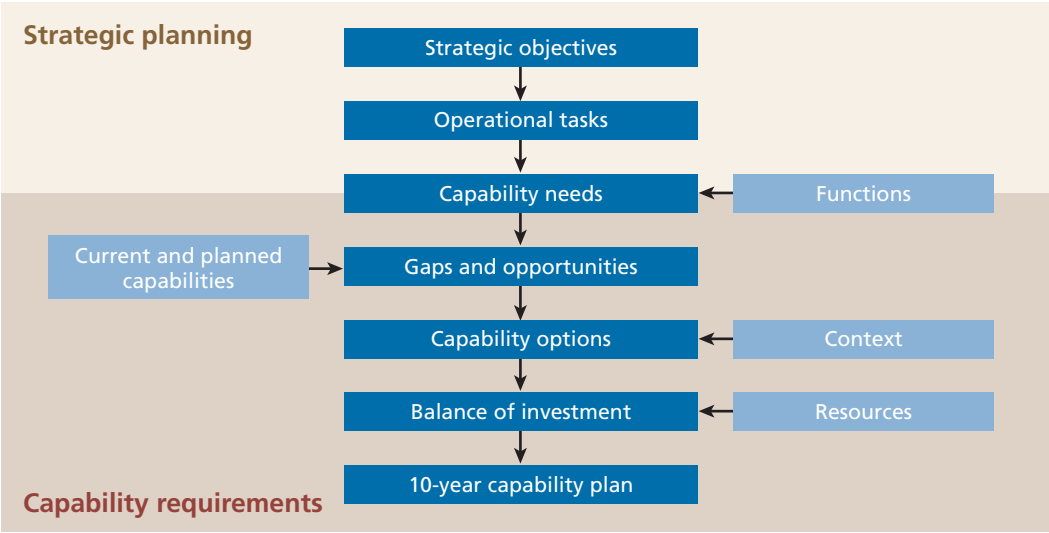
Based on the analysis, RAND researchers developed two logic models for capability identification. The first of these represents best practices (Figure 4.2). However, it is quite complicated, and assumes a level of maturity in terms of the systems, skills, processes and tools that is not currently resident in the Department and ABF. Therefore, it should be treated as aspirational, to be worked toward over time. The second logic model is a feasible interim one that the Department can immediately apply (Figure 4.3). A summary of each step within the capability identification logic model is found below. Detailed descriptions for each step are provided in Appendix G (strategic planning phase) and Appendix H (capability requirements phase).

Figure 4.2
Mature Capability Identification Logic Model



NOTE: Balance of investment = BoI.

Figure 4.3
Interim Capability Identification Logic Model



Strategic Planning Phase

Logic Model

The strategic planning phase (represented in the upper halves of Figures 4.2 and 4.3) aims to develop a strategy-led, auditable process that links government guidance to capability needs through strategic objectives and operational tasks. This is achieved through a capability framework that seeks to minimise strategic risk while exploiting emerging opportunities. In a mature model (Figure 4.2), such as that employed by Defence, it links government guidance, the current and future strategic environment, and Portfolio structural arrangements to identify the capability partitions needed to best achieve the principal tasks that underpin achievement of the strategic objectives.[9]

Linking Strategy to Capability Needs

Strategic planning within the capability development context requires a transparent, auditable and repeatable framework that links government guidance to capabilities needs. We have utilised the commonly used 'strategy-to-task' approach, which links the strategic ends to the operational tasks (means) which, in turn, link to capability sets to achieve these tasks (ways).[10] The upper part of Figure 4.2 provides a mature logic model for this, while the upper part of Figure 4.3 provides a simplified version.

---

[9] De Spiegeleire, 2011, p. 22.

[10] See David E. Thaler, *Strategies to Tasks: A Framework for Linking Means and Ends*, Santa Monica, Calif.: RAND Corporation, MR-300-PAF, 1993.

Noting the relative immaturity in capability development within the Department, the RAND research team suggests employing the simplified approach as an interim model. The Department would employ the mature approach once its capability development processes, systems and capabilities are established. A more detailed description of these logic models, along with some worked examples to tests their viability within the Home Affairs context (based on publicly available information), can be found in Appendix G.2.

The strategic planning phase produces capability sets, which are defined in terms of capability needs (assessed against principal tasks), the risks associated with these capability sets, and the emerging operational environment (see Appendix G.3 for worked examples). Figure 4.4 outlines a simple taxonomy that underpins the strategic planning phase. Using the definition of capability, this analysis considers objectives to be the effects that Home Affairs seeks to generate, with the likelihood that several entities will contribute to achieving an objective.

It is important to note that strategic planning does not operate in isolation of the available resources or external environment.[11] As such, government guidance will determine the resources available and the context within which investment decisions should be made. These resource implications are then considered explicitly in subsequent phases as capability options are developed. The other component of government guidance that flows into the latter phases is the Home Affairs strategic context. This incorporates current security risks, emerging threats, and potential future operational landscapes. While these are explicitly included when developing capability options, they should be considered when defining the strategic and operational objectives, and the operational tasks. The limitation of the simplified model is that these other elements are not explicitly considered.

Figure 4.4
Strategic Planning Taxonomy

Term	Definition
Objectives	Why something should be done
Tasks	What needs to be done to meet the objectives
Functions	The roles the government has asked for
Capabilities	How the tasks will be accomplished

[11] White, 2008.

Capability Requirements Phase

The capability requirements phase (represented in the lower halves of Figures 4.2 and 4.3) results in an identification and risk-based prioritisation of capability gaps and opportunities, an understanding of the operational means of addressing or managing those risks and gaps, the establishment of a 10-year capability plan (i.e., all capabilities including those in service, in acquisition and under development). Each capability, at a minimum, would have made estimates of through-life costs and personnel requirements; identified critical decision points, potential overlaps and interdependencies; and developed a strategy of engaging other departments and government (as necessary). Doing so would ensure that the Department and ABF has a long-term, enterprise, whole-of-life view of its capabilities. To do this, however, the Department would have to recognise that developing capability business cases and sustaining and disposing of capabilities involve significant resource implications.

Logic Model

A mature framework for the capability requirements phase, based on CBP best practices,[12] is shown in the lower half of Figure 4.2 and described in greater detail in Appendix H.2.[13] Establishing the mature model requires a significant investment of resources, particularly up front, as the processes, documentation, systems and corporate knowledge are established. As such, the mature model will require a lengthy rollout period. Given the pressing needs within the Department for a workable capability development approach, the RAND team proposes a simplified logic model (Figure 4.3). This model still aligns with CBP approaches that focus on a singular operational task, while *needs* for that task are linked to *options* and are tested through *mission* (context from our perspective) and *choices* (i.e., the capability plan).[14]

The simplified model can act as an interim approach to meet the needs of the Department and ABF as it develops the staff capacity, corporate knowledge, information systems and analytical tools needed to build and maintain a long-term capability plan. Applying the simplified model affords the Department the opportunity to implement the mature model once the organisation is equipped to do so. The RAND team suggests that could be when Home Affairs decides to undertake a major capability development review, as Defence does periodically. The simplified model would still be suitable for use in the years between these major capability development reviews with each step focusing on adjusting the current elements (i.e., existing gaps and opportunities, options, and resource estimates) in light of changes identified in the strategic planning phase.

---

[12] See Technical Cooperation Program, 2004.

[13] The is based upon the standard CBP approaches (Technical Cooperation Program, 2004) and their application in a Defence context (Australian Government, Department of Defence, 2012a.).

[14] See for instance, Davis, 2002, p. 1.

Capability Gaps and Opportunities

The capability requirements phase commences with the identification of capability gaps and opportunities. The focus is to allow judgements to be made as to whether the Department will have sufficient capabilities over the next ten years to deliver the outcomes and effects to meet its capability needs. This requires assessing how existing and planned capability perform in meeting current and anticipated future needs across at least the next decade. As capabilities reach the end of their use, capability gaps will emerge and must be captured. Advances in technology might also offer opportunities to achieve tasks in previously unattainable ways. Closing all gaps and realising all opportunities are likely to be beyond the capacity of Home Affairs. To manage this, the full set of gaps and opportunities are prioritised using a structured analytical approach, in which comparative assessments are made against a standardised set of risk-based criteria that are derived from strategic and operational drivers.

Capability Roadmaps

Concurrent with this activity is the development of functional sub- (or tier-two) strategies and concepts of operations across the functions identified in the strategic planning phase.[15] Mapping the prioritised gaps and opportunities to functions (via the relevant strategies and concepts)[16] provides the basis for functionally based capability roadmaps that use the prioritised capability goals and the timeline for when they need to inform where likely investment and disinvestment decisions need to be made.

Capability Options

Decisions are then made as to which of the capability priorities are to be explored in greater depth. Best practices recommend the development of broad capability design options for addressing the high-priority gaps and opportunities outlined in the capability roadmap.[17] Creating diverse capability design options allows for the exploration of distinctly different alternatives to addressing a gap or realising an opportunity. Best practices indicate that these options should be described in terms of FIC to avoid a tendency in the Department to focus on materiel solutions (e.g., systems and platforms).[18] These options are tested against an endorsed set of planning scenarios in order to evaluate their relative utility when embedded within the broader enterprise capabilities,

---

[15] For instance, see examples of these for Transport Security in Australian Government, Department of Infrastructure and Regional Development, *Transport Security Outlook to 2025*, 2017b.

[16] Some gaps and opportunities might impact multiple functions. This should be captured, as it may be relevant during the BoI activity.

[17] "Analysis of Alternatives, Cost Estimating and Reporting," in *Defense Acquisition Guidebook*, 2017.

[18] "Program Management," in *Defense Acquisition Guidebook*, 2017.

both those that currently exist and those that are planned. To ensure the feasibility of each capability option, there should be a comparative analysis of each option.[19]

Forecasting resource demands may not be straightforward, as it incorporates both budget and personal requirements—well into the future—for options that are not fully formed. These can be established using analytical approaches such as parametric modelling or trend analysis. A timeline that includes key decision points, such as the retirement date for an existing capability and when government decision is required, is also necessary. A tailored approach can be taken so that projects of lower complexity, risk, or scale can utilise a simpler approach (such as a market survey).

Balance of Investment

Given that Home Affairs represents a complex, interdependent system of cooperative (albeit sometimes competing) capabilities, it is necessary to undertake an enterprise-level cost-benefit analysis. BoI analysis can take a number of forms. The most comprehensive method would be to look across the entirety of the enterprise, including all capabilities. This can be difficult, particularly for the first iteration, as the demarcation between functional areas can be problematic. A better approach would be to allocate resources to each functional area and allow each of them to undertake their own analyses and then focus integration on capabilities that support the same operational tasks. Such an approach provides an opportunity to find synergies, remove inefficiencies, or both.

Capability Plan

Once the options for each capability are agreed upon, these can be integrated into a long-term capability plan. Based on the practices of peer organisations, the RAND team recommends a 10-year plan, as this looks far enough beyond the forward estimates to ensure a comprehensive understanding of the longer-term capability and financial issue, but not too far as to go beyond the lifecycle associated with the planning, acquisition, and disposal of most capabilities relevant to the Department and ABF. Equally, a 10-year plan would provide government with an integrated, long-term view of the investment and capability requirements for Home Affairs in a manner that is consistent with Defence. A view of the capability requirements over this time horizon would give greater insight and certainty about the long-term capability investment needs for Home Affairs and provide transparency and clarity about the costs, priorities and sequencing of investment decisions. It should be noted that a 10-year timeframe aligns with the time horizon employed by similar organisations.

Each new capability option that is selected for the capability plan would be designated with a capability project title, functional area and a CM (at the Senior Executive Service-3 level or equivalent). These designations also would include a brief description

---

[19] See, for instance, "Analysis of Alternatives, Cost Estimating and Reporting," in *Defense Acquisition Guidebook*, 2017; Davis, 2002, p. 3.

of the option that would capture the link to the underlying strategic guidance, any risks associated with it, and a discussion of the evidence base for that choice. Additionally, each capability option would contain an indicative time frame for initiation, key decisions, acquisition, operational use and disposal. Home Affairs might consider selectively using the Smart Buyer approach to assist in developing this information. The research team notes that currently the Department initiates a project once acquisition commences. The team believes this is no longer suitable, as this method fails to recognise the need to take a whole-of-life perspective to project management. As such, the team recommends that Home Affairs follow the approach that Defence takes.

For projects under development or already operational, it is necessary to break out their annual resource implications (by FIC). Those implications then must be tested against the capability plans associated with each enabling capability, to ensure that the financial demands can be met. For new projects, simple modelling that estimates resource implications is necessary. In all cases, the resources should be broken down by phase (i.e., development, acquisition, sustainment, disposal) and their expected funding source. The project description should cover possible overlaps, interoperability issues and opportunities to realise synergies between projects. Further analysis should be undertaken to determine if there are specific risks associated with schedule, interdependencies and capability gaps.

Assurance

Another aspect of the Smart Buyer approach is to govern capability projects by using standard criteria by which Smart Buyer defines and assesses capabilities and their maturity.[20] Table 4.1 represents a set of assurance criteria to determine whether a capability option is mature enough to be considered for the capability plan. These criteria are based upon the descriptions used by Smart Buyer, and can be characterised within a risk-based approach whereby both the enterprise risks (top-down [Strategic Alignment], bottom-up [Operational Alignment] and middle-out [External Constraints]) and project risks (Effects [Benefits Realisation], Technical [Technological Maturity], Cost [Financial Viability] and Schedule) are captured.[21] To meet best practice, risks associated with each capability project should be captured at its initiation and incorporated into the risk register.

[20] See Appendix D for more details.

[21] For instance, Australian Government, Department of Finance, *Implementing the Commonwealth Risk Management Policy – Guidance*, Resource Management Guide 211, 2016a.

Table 4.1
Capability Requirement Phase Assurance Criteria

Criteria	Typical Questions
Strategic alignment	Is the capability requirement consistent with endorsed guidance? Is the scope clearly defined and bounded? How susceptible is it to changes in the strategic environment?
Operational alignment	Is the capability requirement consistent with existing policy, administrative arrangement, and legislation? Is it well aligned with existing organisational functions and priorities? Does it identify and quantify capability inputs?
External constraints	Are there identified external factors (e.g., legislative, administrative) that constrain decisionmaking? Is there a compelling case for these to be developed within the portfolio? Is there sufficient consideration given to coordination across all governments (i.e., national, state, local)?
Benefits realisation	How compelling is the case for the capability, and are the metrics appropriate? Are the benefits sufficient to justify the level of investment? What is the level of confidence that the benefits will be realised over the life of the capability?
Technological maturity	Is there evidence that the technology will mature to meet acquisition timelines? Is there sufficient capacity in the RD&I community to successfully develop the technology? Is the potential for technology redundancy during the life of the capability considered?
Financial viability	Is the proposed funding instrument appropriate? Are the financial figures of an appropriate quality given the maturity of the project proposal? Is the impact of investment on the current integrated investment program well understood?
Schedule	How feasible is the proposed acquisition schedule? How well are the critical path dependencies with other capabilities captured? How flexible are the planned approval and in-service dates?

NOTE: Benefits realisation is not an explicit Smart Buyer criterion, although it is captured under other criteria.

Capability Design Activity

Capability Definition Phase

Capability development acts as the bridge between the aspirational long-term capability plan and the medium-term investment program by establishing an enterprise-level program management environment that prioritises capability requirements into an interrelated set of capability projects.[22] Within the capability definition phase, details are established for each project through the development of initial business case and other supporting documentation, which allows a prioritisation process to inform acquisition decisions and whole-of-life support managed through a multiyear integrated investment program (see Appendix I). The output is a set of prioritised capability projects, described in terms of the desired capability posture, each with an investment approval strategy based on its inherent complexity, an agreed multiyear funding envelope

[22] Australian Government, Department of Home Affairs, "Project Management Framework 'At a Glance,'" version 4.40, internal document, 2018e.

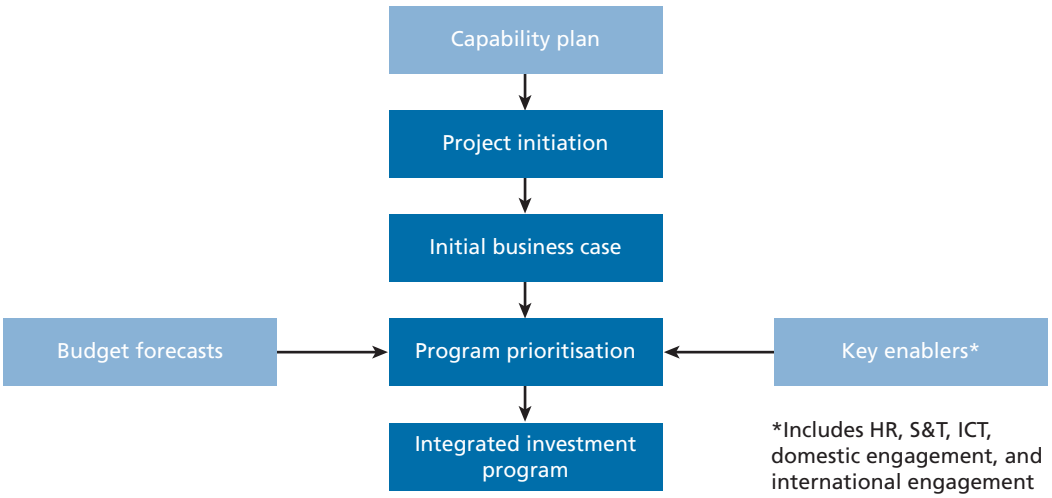
(including estimation of any design, operation, sustainment and disposal costs beyond the investment program), and any interdependencies between projects. Once endorsed, it releases the resources necessary for capability design activities required to establish the proposals for investment approval.

Before proceeding, readers should note that the RAND team's definition of a project differs from that currently used in the Department. Currently, the Department determines that a project only exists within the capability delivery phase (phase 5 of the CLMM) when funding has been allocated. This is not consistent with the practices of similar organisations, and creates unnecessary constraints on managing the capability lifecycle. Initiating the project at the capability development phase recognises that there are resource implications in developing the business case for a capability. It also allows for consistency in terms of approach, provides better opportunities to understanding interdependencies, and removes the risk of stovepipes between projects. Further, it provides continuity across the entirety of the capability lifecycle.

Logic Model

The RAND team suggests a single logic model for the capability definition phase, comprising the four steps depicted by the dark blue boxes in Figure 4.5. Critical to this is the role of CM, who is responsible for overseeing and coordinating across all projects that are assigned to him or her.[23] They would need to satisfy that factors such as HR,

Figure 4.5
Logic Model for Capability Definition Phase



SOURCE: Adapted from Technical Cooperation Program, 2004.

[23] The choice of governance model will dictate if, when and how a CM will continue the role as phases change (see Appendix I).

S&T, ICT and domestic and international engagement have been given due consideration. In developing the logic model for this phase, the research team observed that the Department established a five-year Integrated Investment Plan for financial year (FY) 2018–2019, although it was not followed up with the development of the supporting program of work.[24] While this was not based on a capability plan (the Department identified capability gaps and then prioritised these to establish an investment plan), it does demonstrate the Department has some of the key processes in place.

Project Initiation

The first step in the capability definition phase is project initiation. Building on the information collected in the capability requirements phase, this requires the assigned CM to reconfirm the underlying capability need that the project is to fulfil, identify the project manager, establish the schedule of decision events, list the underlying assumptions and risks, and detail the resources required (including SMEs) to develop the initial business case. The CM would bring the information together in a project management plan.[25]

An important consideration is determining the approach taken for acquisition and the level of project governance required (see Table 4.2). Complex or high-risk projects require special attention, with an experienced and dedicated team to support them. Evidence provided by the Department suggests that such projects are rare within Home Affairs, with a handful of such projects across the entire Portfolio over the life of the capability plan. It is recommended that the Department establish a dedicated central capability, and that the CM augment the team with SMEs from their own functional area. Additionally, the RAND team suggests that the Department consider utilising Defence's Smart Buyer decisionmaking framework to help build internal knowledge and consensus on the project, frame the project to reduce some of the complexity, and initiate and establish the relevant supporting documentation.[26] The CM also may choose to engage the central agencies and any other departments or portfolio agencies that might have a material interest, both to provide them with early awareness and to allow considerations raised by them to be considered.

---

[24] We use the word 'program' rather than 'plan' here, to emphasise the certainty provided by gaining government approval. Thus, it becomes a program of work with funding guidance, rather than a plan.

[25] See, for example, Australian Government, Department of Defence, 2012a, p. 48.

[26] We note that Home Affairs has initiated discussion with Defence on utilising the Smart Buyer framework.

Table 4.2
Capability Project Types

Project Type	Typical Characteristics	Governance Approach
Major	• High cost, high risk, high visibility, high technical complexity, high contractual complexity, or some combination thereof • Unique or bespoke capability that requires knowledge and skills beyond those resident within the department • Can represent a new capability for the portfolio • Significant interdependency and interoperability issues, particularly with other departments	• Establishment of project team with membership representative of the stakeholder group (including from outside the department) • Initiate through the Smart Buyer program or a similar approach • Expectation for multiple passes though government approval to minimise project risk • Delivered through a centralised capability, augmented by external service providers • Monthly reporting to senior executive • Early engagement with central agencies • Independent cost assurance may be necessary
Standard	• Medium acquisition cost, medium risk, medium visibility, medium technical complexity, medium contractual complexity, or some combination thereof • Operational and sustainment costs are manageable in the long-term • Capability solution typical to a functional area • Interdependency and interoperability issues managed internally	• Establishment of project team with membership from operator, acquisition, and development areas • Initiate through the Smart Buyer program or a similar but simplified internal approach • Two-pass government approval, with first pass being inclusion in the investment program and second pass being investment approval • Capability development and acquisition expertise provided internally through a centralised capability, augmented by operators • Quarterly reporting to senior executive (or by exception)
Omnibus	• Aggregation of small interdependent projects that are similar in nature and at medium or below levels of cost, risk and contractual complexity • Dynamic development environment with high rates of technology evolution • Operational and sustainment costs are manageable in the medium term • Aggregation allows flexibility in the order and delivery of the overall capability • Able to be effectively managed within a functional area	• Managed within a functional area by the CM • Funding provided as the total for all contributing projects • Flexibility in delivery of individual components while the project remains within expenditure boundaries and meets targets agreed to within business case • Annual reporting to executive (or by exception)

Project Type	Typical Characteristics	Governance Approach
Simple	• Capabilities which represent an incremental improvement over time, and where there are low levels of risk and contractual or technical complexity • Able to be effectively managed within a functional area • No significant changes to sustainment and operational costs	• Managed within a functional area by the CM • Annual reporting to executive (or by exception)

Initial Business Case Development

The approach Home Affairs currently employs to develop business cases for projects is appropriate, and aligns closely with that employed elsewhere in government in Australia and elsewhere.[27] However, the RAND team's interviews with Department and ABF staff and its review of some DIBP business cases indicate an inconsistency in input, both in terms of quality and completeness. There was also the suggestion that the level of detail expected for initial business cases was unnecessary. The level of detail required of the initial business case should reflect the complexity of the project (see Table 4.2) and have sufficient information to support prioritisation across the program. In developing the processes and tools for implementing the capability development, the Department should simplify initial business case information requirements (Table 4.3).

Prioritisation and the Integrated Investment Program

Having developed initial business cases for all approved new projects, the next step is to establish which projects will be developed further, over what time frame, and using which funding instruments.[28] Using the Department and Portfolio finance plans, a determination can be made as to how much funding is available over the forward estimates. Anticipating the total funding required to support the preferred option for all projects, a risk-based mechanism to optimise the program will be necessary. Other constraints such as workforce number (including skill and competency requirements), infrastructure requirements and ICT demands would also be included. It is critical that CMs represent the projects under them during this process. The approach to optimisation should lead to a negotiated solution that is based on overall organisational needs, rather than balancing investment across the functional areas.

The first step would be to determine whether to disinvest and amend any projects that are listed on the investment program but have yet to commence acquisition. The remaining projects would then be optimised globally to determine the best coverage

[27] See, for example, Australian Government, Department of Defence, 2012a, p. 55.

[28] It is assumed here that while the Portfolio capital budget is approved on a year-by-year basis in response to the government's budget priorities, that once a project is approved for funding under this mechanism, it does not need to seek reapproval each year, other than by exception.

Table 4.3
Baseline Requirements for Initial Business Cases

Element	Description
Title and descriptor	The name and descriptor naming convention for the capability project
Establishment of the context	An explicit link to the strategic objectives, capability gaps and opportunities, the capability requirement, and the implications for taking no action
Summary of capability options	A description, advantages and disadvantages associated with the option, an FIC analysis, a decision schedule, an annual budget estimate for acquisition and sustainment, and discussion of financial instruments
Project management complexity	The choice of which project management approach will be employed and the basis for this
Key risks	For each option; would include enterprise, technical and project risks, their level, and potential mitigations
Interdependency and interoperability issues	This includes identifying dependencies between each option and other existing and planning capabilities, future gaps that impact the option, and other demands on the resources required for the operation and sustainment of this capability option
Recommended option	A comparative analysis between proposed options, made against capability requirements, as a basis for the preferred option
Supporting evidence	The evidence base and associated analysis that underpins the options selected, and the recommendation for the preferred option
Internal stakeholder viewpoints	Includes capturing the perspectives of key internal stakeholders, such as the Finance Group, the People Group, the ICT Group, the operator community, those responsible for acquisition and sustainment, and infrastructure; the aim is not to achieve consensus, but rather to ensure all viewpoints are considered prior to a decision being made
Engagement strategy	Outline of engagement requirements with other departments and agencies that might directly support the acquisition and sustainment of the capability, and the time and nature of engagement with the central agencies
Industry capability	Includes the level of industry support required, the maturity of the marketplace, and strategy for engaging industry (if required)

of capability gaps and opportunities, given the available resources. This might require selection of nonpreferred but lower-cost options to provide better coverage of a gap. Alternatively, a risk strategy that seeks the broadest coverage of gaps might accept a capability that is less effective against a single, but higher-priority, gap. The outcome of capability definition phase is a five-year Integrated Investment Program which would be sent to government for approval. Once approved, it provides the Department and ABF with a level of funding certainty with which to develop and deliver the capabilities that the Australian government requires.

Assurance

As noted previously, the Department established a five-year integrated investment plan for FY 2018–2019. However, we observe some issues that suggest the project assurance for the capability definition phase requires some attention. It was unclear whether dedicated resources were allocated to this phase, although it appears that when this did occur, the resources were taken from operational funds and might not have been sufficient. We also observe that the plan was not adhered to when it came to investment decisions, nor was it clear that a program of work was established. We cannot be definitive in explaining why this was the case. However, interviewees suggested that those changes may have been due to the establishment of the Department, or that some areas within the new Department made the determination that some of the agreed priorities were not necessary. This emphasises the importance of shared decisionmaking among senior management, appropriate responsibility and accountability for those charged with delivering the capability to the operator community, and an empowered assurance function to ensure that the integrity of an investment program is maintained. Those providing the assurance function should not actively participate in the program prioritisation activity, but rather should help with facilitation and arbitration. In essence, managers would provide quality assurance through an audit of the integrated investment program, typically asking similar questions to the capability requirements phase.

Investment Approval Phase

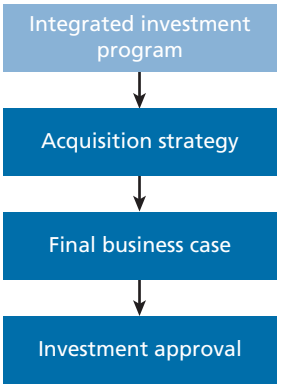
Logic Model

Within the Department, the investment approval phase of the CLMM is the most mature of the four phases considered within this report. There is a standardised template for developing business cases and a consistent approach for determining whether to seek additional funds (i.e., NPPs). There is a formal mechanism for engaging internal and external stakeholders, albeit sometimes later than what is ideal, and there is a governance structure to oversee the process. This is not to say that there are not areas for improvement, nor that the Department and ABF always adheres to the application of the approach for investment approval. Certainly, comments from interviewees identified some concerns. However, the overarching approach is sufficient to support an effective CLMM, and aligns with approaches applied in similar circumstances.[29] In spite of this, it is incumbent to identify a straightforward approach that utilises the strengths of the current Department process, so as to ensure there is a level of consistency within and across Home Affairs.

The RAND analysis has identified three steps for the investment approval phase. These are shown as dark blue boxes in Figure 4.6 and outlined below.

[29] For instance, Defence and U.S. DHS.

Figure 4.6
Logic Model for Investment Approval Phase



Acquisition Strategy

With government approval of the integrated investment program, the Department is able to plan the acquisition of capabilities with a level of financial security, notwithstanding the fact that government may still need to approve any capability proposals that require additional funds, such as an NPP. Given this conditional approval for a project to proceed, the investment approval phase commences by using the initial business case (see Figure 4.5) as the basis for determining the most efficient and effective approach to the acquisition of the underlying capability. This must include all FIC elements and distinguish where those elements can be provided through existing internal resources (e.g., staff with the necessary skills and knowledge), those that require internal investment to realise (e.g., building internal capacity through learning and development), and those that need to be acquired from external sources. This forms the basis of the acquisition strategy, which must look more broadly than the purchase of a given platform or system. The strategy should extend beyond what is to be acquired and determine how that acquisition will occur. Internal documentation, such as a HR strategy, will assist. For those elements that are expected to come from external sources, a review of the market is necessary to understand the private sector's capacity, potential vendors, price points and other underlying commercial issues (e.g., constraints on providers for certain types of ICT equipment). Typically, a 'Request for Proposal' or similar instrument can be used to sample the marketplace.

Final Business Case

Having established their strategy for acquisition, the CM and the appointed project manager would use this with the initial business case to develop the final business case. Having reviewed a number of final business cases across Home Affairs, the RAND team observed that the current template used within the Department captures most of the key elements. However, the team identified inconsistencies between proposals and

gaps within the template. These are summarised in Table 4.4, and represent a modest adjustment to the current template that would do the following:

Table 4.4
Review of Home Affairs Business Cases

Component	Included in template?	Comment
Proposal description	Yes	This should be a short summary of capability that is being sought, taken from the initial business case.
Business problem or opportunity	Yes, but should be renamed 'capability gap or opportunity', consistent with current Home Affairs language	This should be the capability gap or opportunity identified in the capability definition phase.
Objectives and outcomes	Yes, but should specify operational objective or outcome in the mature model	This should provide the underpinning strategic driver for the capability. The reviewed business cases often link solely to strategic outcomes and objectives. As a discriminating factor, this is too high-level. Therefore, under the mature model, operational objectives should be used.
Operational tasks	No	The inclusion of operational tasks provides a clear and measurable statement of what of a capability might need (e.g., 'deter, disrupt, detect and investigate the unauthorised trade across the border continuum').
Impact of not proceeding (do-nothing option)	Yes	This is a statement of risk, and should be cast in terms of impact on operational tasks of the capability gap or opportunity not be addressed by this capability proposal. If there are other existing or proposed capabilities that can (in part at least) address the gap, that should be included.
Recommended option or alternate option	Yes	These are two sections with 12 subsections. There is benefit in having a statement on why the options were selected, a comparative analysis of each (including funding, timelines, FIC implications and risks), and a statement on why the recommended option is preferred (including a summary of the supporting evidence). The details in the subcomponents would each be an annex to the main document. The template should not be limited to two options.
Options annex	No, however, the subsections for each option capture this	The 12 subsections, as they stand, are sufficient. However, the resources and financial implications must include sustainment and disposal costs, and there should be an analysis against each FIC component. Clear statements need to be made—regarding interdependencies and interoperability with other existing or proposed capabilities—as a separate subsection. Finally, key stakeholders outside of Home Affairs, industry capacity and the evidence base need to be captured.

SOURCE: Based on the current Home Affairs *Business Case* template. (Australian Government, Department of Home Affairs *Business Case Template*, version 3.5, internal document, 2018g.)

- provide a clear linkage to the underpinning strategic drivers, operational objectives and operational tasks that will enable Home Affairs to improve reporting to government
- ensure that both the internal and external resource requirements are identified throughout the lifecycle of the capability
- provide an evidence base that explains why the option set was chosen and the case for the preferred option
- consistently define capability in terms of effects and FIC
- ensure that risks associated with the capability proposal (including of not proceeding with the proposal) are known, and can be monitored through the lifecycle of the capability.

Investment Approval

Based on the timeline agreed in the integrated investment program, the final business cases would then be tabled for discussion at the appropriate internal committees. These committees would review the proposal and agree which option (if any) to proceed with. Projects seeking external funding would need to be reviewed by the Executive Committee, before proceeding to government for approval. For internal projects, a threshold requiring only the approval of a lower-level committee could be established to determine approval to proceed to the Department's most senior committee. Under the current committee structure, a proposal falling under the immigration functional area would go to the Immigration Report Steering Committee. With this final acquisition approval, Home Affairs could take an approach to market (such as through a request for tender) and then to acquisition. Key documents, such as operation concept documents and functional and performance specifications would be developed to support the request for tender.[30] Once the tender evaluation is completed, plans for acquisition and sustainment and disposal for the capability would be developed and integrated back into the capability plan and integrated investment program. In select cases, such as complex or high-risk projects, it may be determined that a two-pass government approach is necessary. In such cases, further government approval occurs once the tender evaluation process is completed.

Key Decision Points

As Defence determined through the *First Principles Review*, efficiencies can be gained by tailoring required body of knowledge so that it is sufficient to make an informed decision. As such, it is important to ensure that proposals reaching decision points between phases in the CLMM are tailored accordingly. Applying the Home Affairs

[30] See, for instance, Australian Government, Department of Defence, 2012a.

Table 4.5
Proposal Requirements at Decision Points

Components	Capability Plan	Investment Program	Project Approval	Comment
Business case	No	Indicative	Detailed	This should include capability options described in terms of FIC, and should provide a comparative analysis of those options. It is likely to contain much of the other information identified in the Project Management Framework.
Purpose, definition and approach	Yes	Yes	Yes	This should remain consistent throughout, and explicitly link to strategic guidance through needs (gaps and opportunities), tasks and objectives. A definition of the capability should be included.
Risk management	Yes	Yes	Yes	A risk register should be established, maintained, and reviewed throughout the project. Schedule, cost, and technical and capability risks should be identified.
Interdependencies	Yes	Yes	Yes	These should be assessed and incorporated into the risk management plan. Implications for resources, schedule and capability should be noted.
Schedule	Indicative	Key decision points	Detailed	Risks to the schedule and potential implications for other projects should be identified.
Finance and budget	Estimate	Improved estimate	Detailed	This must be for the whole-of-life of the capability, including the cost to develop capability plans, acquisition, operations, sustainment and disposal.
Resource management	Estimate	Improved estimate	Detailed	This is initially assessed in terms of relative difference by with increasing detail. By the project approval phase, this should include numbers, skills, and levels, and associated offsets elsewhere (as necessary).
Quality management	No	Yes	Yes	This would include a formal plan for evaluating quality throughout the life of the project.
Project team	Yes	Yes	Yes	The CM and project lead need to be identified once a project is initiated. In general, the team will consist of operator SMEs and those experienced in the practice of capability development. Depending on project complexity, external providers and representatives from other departments might also be members.

Project Management Framework to each of these components (e.g., the business case), the RAND team recommends the following as the minimum requirement at the key decision points for phases 2 through 4 of the CLMM (see Table 4.5), namely

- the 10-year capability plan (capability requirements phase)
- the 5-year investment program (capability definition phase)
- individual project approval (investment approval phase).

Annual Planning Cycle

Finally, it is important to situate the entire lifecycle within the annual planning cycle that all government departments must adhere to. Importantly, we suggest that Home Affairs follows approaches similar to those employed in similar organisations (e.g., Defence). This entails two distinct programs of activities. The first of these programs of activities entails a dedicated, detailed planning activity that occurs as the result of major changes. For instance, a major review might occur every four years. However, the decision to undertake the major review will generally be driven by factors external to the Portfolio. By way of example, Defence performs such an activity in the lead-up to publishing a white paper. This activity is resource-intensive and would require providing additional resources (e.g., SMEs, funding for studies) to the organisational unit dedicated to managing the first four phases of the CLMM.

Between these major reviews, the Department could undertake a second program of activities that would deliver an annual update so as to allow for in-course adjustments to the detailed plan. The activities necessary to undertake this would be an abridged version of those undertaken for a major review. In the opinion of the RAND research team, this represents business as usual for the unit managing CLMM. Given the relative immaturity in capability development within the Department, the research team suggests that the Home Affairs might choose to use an abridged update cycle for the first one or two years to help build the knowledge and skills of those managing, allow time to build the data and tools necessary to support it, and reduce the burden on the Department. It is worth noting that the Victoria Police elected to take a similar approach when they were rolling out their CBP system, and initially focused only on forensics.

Testing the Model

Having developed the capability development model, RAND's research team sought to explore its feasibility. To do this, researchers undertook a series of semistructured discussions with Departmental and ABF staff who had experience in capability development and acquisition. The intent was to determine if and how the model would have impacted the development and delivery of those projects if it had existed when they were initiated. These test cases were focused on a range of capabilities that cor-

Table 4.6
Test-Case Observations

Test Case	Nature of Project
Project management office	While not a project *per se*, this area has experience in providing project management and delivery support across the Department.
SmartGate	Represents an example of a standard project which had some later issues. Allows a discussion on whether the model could have mitigated those.
Aviation security	Represents an example of a standard project that has to balance short- and long-term needs, and where business continuity can limit sustainment and business continuity.
Future Maritime Surveillance Capability	Represents a major project that is bespoke for Home Affairs, and where the technical skill required will not be resident in the Department and ABF. It also requires significant engagement with external agencies both from a financial and capability perspective.
UHF radios	Represents a project that seeks to coordinate similar needs from across Portfolio agencies and where the technical skills are not resident. Some level of external engagement is necessary, given the communication spectrum.
Enhanced data warehouse	Represents an example of a foreseeable ongoing requirement which transcends the organisation, and which can face new challenges at short notice.
HR: integrated job roles	Represents a test case of an enabling capability area which needs to also build its own capabilities.
Visa: systems for people	Represents an example of an omnibus project which contains tranches of activities that are to be delivered on a regular basis.

responded with the spectrum of projects within the Department. The project's aim was not to explore those examples in detail, but rather to use them as a basis to think through the model. The summary of the test cases can be found in Table 4.6.

The discussions progressed through a definitional element (including defining the principles), then each of the four phases, and finally looked at the nature of governance. In all cases, there were no major impediments with the model, and minor issues (often language) have been adjusted. Comments from the Department staff were consistent with those expressed in the initial interviews; these comments also reinforced what the research team learned about experiences in other organisations (see Chapter Two). The test cases generally supported the principles and reinforced the notion that the model is feasible. Nevertheless, they raised the following issues that might need consideration during implementation:

- It is critical to have a clear linkage between high-level strategy and capability decisions. A missing piece is often the tier-two strategies.

- Incorporating whole-of-life costings is critical, otherwise the Department risks selecting capability options with lower acquisition costs but higher operational and sustainment costs.
- By having a long-term capability plan linked to a medium-term investment program, the Department can plan and operate more strategically. It can provide the basis for engaging earlier, explaining the basis for the business case better, and explaining the consequences of changes in government policy or short-term demands. This would also help with disinvestment.
- Projects cannot be treated in isolation. The links across the program are important, especially if there are opportunities to get global optimisation that might actually require individual projects to choose a less optimal option.
- Participants support a tailored approach to projects based on complexity. Further analysis may be required to clearly establish boundaries and policy settings.
- Implementing a governance model that is known, empowers individuals and holds people accountable is critical. Decisionmaking via committee process is useful from a consultative perspective, but it sometimes leads to situations where no single individual is ultimately responsible.
- Participants strongly supported a CM role. However, such a role must be empowered and resourced, and the individual must be appropriately skilled to perform the function effectively.
- Participants endorsed the establishment of a functional area to support capability identification and design functions. In particular, workshop participants cited the need for whole-of-system analyses, especially to help decision-makers understand how to balance investments.
- There is a need for formal and on-the-job training and development of all staff involved in capability development.
- While the project areas demonstrated deep knowledge of the capability areas, some participants noted a lack of some the specialist skills necessary to support business case development, contract management and technology evaluation. The participants suggested that the Department consider building an internal capability, from which project areas can access these skills and develop the capacity to procure specialist skills in narrow areas.
- Consistency in terminology and a standard lexicon are important and need to be endorsed.

CHAPTER FIVE

Governance Model Options

As noted in Chapter Two, a key finding from the RAND research team is that there would be benefit from creating governance structures that are tailored to the complexity, size and risk of each program, to give capability development programs greater agility and assurance. This chapter examines the attributes of three governance models that could be employed to mature the Home Affairs capability development process. The chapter then goes on to examine the ability to tailor such governance models.

Governance Best Practice

In 2007, the Australian Public Service Commission (APSC) noted that a key challenge for public servants is 'understanding the full responsibilities of good governance'.[1] Equally as important as the 'must-do' elements of governance (e.g., adherence to government oversight and accountability) are the 'should-do' elements of governance (e.g., organisational culture). The APSC notes that these elements 'must be actively upheld and implemented by every person in the organisation. Everyone must know and act on their responsibilities'.[2]

Based on analysis of Australian and international governance frameworks (see Appendix J), the RAND team recommends that the governance structures within Home Affairs be underpinned by the following principles:

- **Accountability:** being held to account for decisions made, and having meaningful mechanisms in place to ensure the agency adheres to all applicable standards.
- **Transparency/openness:** having clear roles and responsibilities and clear procedures for making decisions and exercising power.
- **Integrity:** acting impartially, ethically and in the interests of the agency, and not misusing information acquired through a position of trust.

[1] Australian Government, *Building Better Governance*, Australian Public Service Commission, 2007.

[2] Australian Government, 2007.

- **Stewardship:** using every opportunity to enhance the value of public assets and institutions that have been entrusted to the Department's care.
- **Efficiency:** ensuring the best use of resources to further the aims of the organisation, with a commitment to evidence-based strategies for improvement.
- **Effectiveness:** bringing a wide range of relevant experience to bear, including through offering rigorous challenges and scrutinising organisational performance.
- **Leadership:** achieving an agency-wide commitment to good governance through leadership from the top.
- **Teamwork:** fostering a collaborative workplace, communicating openly, solving problems in a collegial manner, sharing ideas, and taking advantage of the diversity of knowledge and experience among staff.
- **Sustainability:** taking a long-term view about what the Department is trying to achieve and what it is doing to get there.

Proposed Governance Models

Our interviews, literature reviews and analysis informed the development of three distinct governance models options. While these models can be treated as being independent, the research team notes that the optimal choice may be a hybrid of them, in light of statutory responsibilities, security constraints or constrained funding instruments. Appendix K provides a detailed review of these models.

A number of functions and roles cut across these models. The role of CM is particularly important,[3] as the CM is responsible for identifying specific capability needs and requirements, including FIC. The CM maintains a pipeline of potential new capability projects which are under consideration. In practice, the CM should be from or very closely aligned to the operational agency (e.g., ABF). A CM is required for each key Home Affairs capability domain.[4] These domains might be defined along organisational lines (as occurs in Defence) or functional lines (as occurs in the UK national security environment).[5]

Centralised Governance Model

The Centralised Governance Model was derived from the capability development model employed by Defence from 2003 to 2016. During that time, Defence created two organisational functions to support this: the Capability Development Group was responsible for the capability requirements to investment approval stages, and the

[3] Victoria Police use the term 'capability stewardship' when describing their equivalent function.

[4] Australian Government, Department of Defence, 2015, pp. 5, 18.

[5] United Kingdom Government, Cabinet Office, *National Security Capability Review*, March 2018a.

Defence Materiel Organisation was responsible for the capability delivery through to the capability disposal stages of the CLMM (see Appendix K.1 for more details).

In this model, one entity is responsible for strategic planning, capability requirements, capability definition and investment approval, while a different entity is responsible for capability delivery, sustainment and disposal. The Centralised Governance Model emphasizes that the skills and knowledge required to develop and undertake the planning elements of the CLMM (phases 1 through 4) are fundamentally different from those required for the delivery, management and disposal elements (phases 5 through 7), and, as a result, there may be benefits to building these areas of expertise separately. However, this risks creating disconnects between the CM, the capability development manager and the delivery agent.

Semicentralised Governance Model

The semicentralised governance model is a centralised model where the CM (generally the operator) has responsibility for the capability identifications phases of the CLMM (see Appendix K.2). A separate delivery agent is responsible for the acquisition and through-life support elements of the capability.[6] A third entity is responsible for the capability design phases. This model ensures that the authority responsible for acquisition also oversees the through-life support elements. This continuity of responsibility produces a range of benefits. It ensures that skills and knowledge reside in a single area. It offers the opportunity to build a more direct relationship with central agencies not only through the investment approval process, but through improved understanding of interoperability issues, enhanced buying power, and the establishment of consistent policies and practices throughout the life of the project. Finally, it allows for greater flexibility for the deployment of staff across projects.

However, under the semicentralised governance model, the CM may have accountability but not responsibility for the delivery of the nonpersonnel-related aspects of the capability. The organisational separation, and possible physical separation, of the CM from the delivery agent could result in tension between the organisations, as a result of their differing drivers. To succeed, this model requires that SMEs from the CM's organisation be embedded in the delivery agent's organisation.

Decentralised Governance Model

The decentralised governance model is similar to the model currently employed within the Portfolio, where each CM is responsible for all stages of the CLMM (see Appendix K.3). However, the CM would come from the organisation that owns the capability, and thus where decisionmaking during its development is taking place. Typically, this

[6] It should be noted that the responsibility discussed here is for the nonpersonnel aspects of the capability.

will be an agency, although it does not preclude a CM coming from the Department.[7] The decentralised governance model allows for a stronger relationship between the operators and the decisionmakers, and for prioritisation to occur in accordance with the needs of the agency rather than the overarching Portfolio priorities. It also reinforces the authorities of the agencies and their resource allocation.

However, this model has a number of drawbacks. Not only does it use resources inefficiently, it also reduces the pool of experts available to undertake such work, limits opportunities for developing interoperable capabilities, and constrains the buying power of the Portfolio agencies. Additionally, this model could make coordination with central agencies more challenging, as the central agencies would be required to engage with multiple stakeholders within the Portfolio. This coordination could be further complicated by the resource limitations within the central agencies. In addition, the opportunity for collecting similar (often small) projects into a single omnibus submission to meet the key thresholds for decisionmaking (e.g., for NPPs) will be lost.

It is noted that this approach does not require division of responsibilities to be structured along agency lines. The Department's four coordinator roles,[8] along with intelligence coordination (through the recently established Office of National Intelligence within the Department of the Prime Minister and Cabinet [PM&C])[9] represent one such framework. It also should be noted that, within the Australian Intelligence Community, there are plans to establish a funding instrument and prioritisation process that incorporates all federal intelligence entities. Similarly, the UK government is establishing interportfolio planning and management for biometrics and cybersecurity.

Summary

The preceding sections identified three governance models for capability lifecycle management within the Home Affairs context, which can be summarised as follows:

- **Centralised governance:** where responsibility for all four capability development phases of the CLMM resides with a single entity within the Department. The remaining three phases of the CLMM are delivered by a separate organisational entity.

---

[7] The UK Government partitions along functional lines (see United Kingdom Government, Cabinet Office, 2018a).

[8] The Department is responsible for providing national coordination of four crosscutting areas, each led by a national coordinator or advisor. The areas are counterterrorism; cybersecurity; transnational, serious, and organised crime; and countering foreign interference (see Australian Government, Department of Home Affairs, 2018a, p. 23).

[9] See Australian Government, Office of National Intelligence, "Overview," webpage, undated.

- **Semicentralised governance:** where the strategic planning phase is provided by one entity within the Department, and all remaining capability development phases and follow-on phases are delivered by a separate entity within the Department.
- **Decentralised governance:** where the Portfolio agencies develop, deliver and sustain their own capabilities.

These options emphasize differing levels of centralisation and the role of the CM. They offer alternatives to how the Department and ABF may choose to progress, though implications for organisational structure, staffing and roles and responsibilities are not addressed.

At the time of writing, data about the volume, cost and type of capability development program currently conducted within Home Affairs were not available. As such, the discussion focused on the key characteristics that should be considered when choosing a governance model, rather than recommending an option. Table 5.1 summarises the differences between the three models.

Table 5.1
Comparison of Governance Models

Centralised	Semicentralised	Decentralised
Accountability and responsibility for every aspect of the CLMM sits centrally. The CM may see requirements change throughout the process.	Accountability and responsibility for the capability requirements phase is with the CM; all other accountabilities and responsibilities are with a single, central group.	Accountability and responsibility for every aspect of the CLMM sits within one agency.
There can be disconnects between the capability development manager and delivery agent.	It is unlikely for there to be a disconnect between the capability development manager and delivery agent.	This model reinforces the authorities of the agencies and their resource allocation. Oversight may be reduced, as all governance takes place inside an individual agency.
This allows for more strategic engagement with centralised agencies and government, and allows for omnibus submissions to government.	This allows more strategic engagement with centralised agencies and government, and allows for omnibus submissions to government.	This allows a more direct case to be made to government, based on specific agency requirements. Coordination may be more challenging due to resource limitations within the central agencies.
This offers an efficient use of resources and capability development decisionmaking, with opportunities for rationalisation across capability areas. There are opportunities for interoperability considerations between projects, as projects are managed from a single area.	This offers an efficient use of resources and capability development decisionmaking, with opportunities for rationalisation across capability areas. There are opportunities for interoperability considerations between projects, as projects are managed from a single area.	This model is a less efficient use of resources. Capabilities are less likely to be interoperable between agencies.

Centralised	Semicentralised	Decentralised
There are opportunities for greater buying power and project coordination, as projects are managed from a single group.	There are opportunities for greater buying power and project coordination, as projects are managed from a single group.	There is lower efficiency, given less coordination between similar projects in different agencies and reduced buying power.
Skill sets can be specialised within capability requirements, contracts, and sustainment, allowing for surge capacity on projects, if required.	Skill sets can be built within one area, allowing for surge capacity across the program. Skill sets between capability requirements, contracting and sustainment are not easily transferrable.	There will be fewer capability lifecycle experts to address requirements, which could challenge surge capacity and the ability to specialise.
The physical separation of SMEs from capability decisionmakers could deliver less-informed decisions due to reduced familiarity with the detail requirements for each capability.	The physical separation of SMEs from capability decisionmakers could deliver less-informed decisions, due to reduced familiarity with the detail requirements for each capability.	There is a greater relationship between the operators and the decisionmakers.
There are opportunities for consistent policies across the Portfolio, with projects being managed from a single area.	There are opportunities for consistent policies across the Portfolio, with projects being managed from a single area.	Policy can be tailored to the specific needs and authorities of the agency.
Robust prioritisation between projects is needed to ensure that every CM receives the capabilities they need.	Robust prioritisation between projects is needed to ensure that every CM receives the capabilities they need.	Prioritisation can occur in accordance with the needs of the agency, rather than those of the Portfolio.

CHAPTER SIX

Implementing the Capability Development Model

This chapter reviews the proposed capability development model that was depicted in Figure 4.1 to determine the implications for Home Affairs in order to support its implementation. We review capability development functions in peer organisations and reflect on the model as proposed. From this, we identify the requirements for a capability development enabling function and the activities that it would perform.

Examples of Capability Development Functions

This section will examine the capability development functions performed within Defence, Victoria Police and the U.S. DHS (see Appendix L). The frameworks employed within these organisations will then be used to provide an overview of the functions that Home Affairs could perform for each of the first four phases of the CLMM.

Defence's Force Design Division

As a result of the *First Principles Review*, Defence established the Force Design Division (FDD) within the VCDF Group. Its function focuses both on the design of current Defence capabilities ('test the force in being')[1] and the requirements for future capabilities ('design and guide the development of a balanced and affordable future force').[2] FDD consists of the following three branches:[3]

- **Force Options and Plans:** focusses on force options testing, force structure planning, and prioritisation.
- **Investment Portfolio Management:** focusses on investment management, performance measurement, and governance.

---

[1] Australian Government, Department of Defence, "Force Design Division," webpage, undated-b .

[2] Australian Government, Department of Defence, undated-b.

[3] Australian Government, Department of Defence, "Force Options and Plans," presentation to the 2017 Force Design Conference, 2017c.

- **Joint Force Analysis:** focuses on concepts, doctrine, lessons and preparedness.

The analysis below will focus on the role of FDD in the development and testing of capability options at the enterprise level, and the smooth transition of capabilities into the Australian Defence Force. This focus has been chosen because it is of particular relevance to Home Affairs. The challenges faced by FDD within these areas closely align with the challenges facing Home Affairs as it seeks to take a more strategic and forward-looking perspective, while simultaneously continuing to maintain operational capability to respond to immediate problems.

The Force Options and Plans Branch contains many of the functions Home Affairs requires to enable capability development and inform investment decisions. Advice from within the branch indicates that it has 28 substantive staff, comprising nine Military Officers, 15 Australian Public Service staff, and four Defence Science and Technology (DST) Group embedded analysts.[4] The functions delivered within the Force Options and Plans Branch include the following:[5]

- managing the enterprise-level capability design cycle
- leading the capability assessment program
- supporting integrated investment program decisionmaking
- developing, exploring and assessing capability options
- undertaking force structure assessments to inform future force design
- analysing, synthesising and prioritising force design outputs
- delivering prioritised and viable portfolio options.

Capability Acquisition and Sustainment Group

While CASG supports all phases of the capability lifecycle, we will focus on the support CASG provides to the first four phases of the CLMM. CASG divides its activities in support to these phases into two broad categories: strategy and concepts, and risk mitigation and requirement-setting.[6] The group's responsibilities in these areas break down as follows:

- **Strategy and concepts**
  - support needs development, especially technical and commercial factors
  - develop initial project risk profiles and project execution strategies
  - coordinate early industry involvement

[4] As of 24 September 2018. The Investment Portfolio Management Branch is of a similar size to the Force Options and Planning Branch, and supports committees and portfolio governance, coordination and measurement.

[5] Australian Government, Department of Defence, 2017c.

[6] Australian Government, Department of Defence, *The CASG Business Framework*, 2017b.

- **Risk mitigation and requirement-setting**
  - develop an executable, affordable integrated project management plan
  - identify and manage risks to the plan
  - plan for sustainment and disposal
  - coordinate industry engagement
  - work with the CM to develop requirements from their needs
  - manage tendering and tender evaluation
  - support the development of business cases by CMs.

We also note that CASG has established six functional Centres of Expertise, of which four are particularly relevant to capability development within Home Affairs, namely the following: [7]

- **Program Management:** includes coordinating FIC, independent assurance and a standardised approach to program management.
- **Engineering and Technical:** includes planning, requirements analysis, and definition activities in support of acquisition and sustainment.
- **Decision Support:** includes reporting of performance, provides stewardship of management support systems and decisionmaking tools, and oversees internal information management.
- **Corporate Performance:** provides standardised governance and management of corporate functions including governance; administration; work, health and safety; and professionalism and capacity management.

Victoria Police

Victoria Police has made a significant investment in capability planning, knowing that it will reshape how it operates and improves the support it provides to the Victorian community. Under its approach, Victoria Police is seeking to establish a system that focuses on the integration between policies, legislation and capabilities. The system employed by Victoria Police places the development and sustainment of capabilities on an equal footing with each other; aligns capability needs with current and future demands; encourages an environment of innovation and continuous improvement; seeks opportunities to streamline internal processes; and aligns strategy, business planning and policy.[8] While Victoria Police does not explicitly state the functions it is developing, it does indicate some drivers for these functions, including the following:[9]

---

[7] See Australian Government, Department of Defence, 2017b. The remaining Centres of Expertise are materiel logistics and commercial.

[8] Victoria Police, 2016, p. 15.

[9] Victoria Police, 2016, p. 5.

- assessing capability maturity to identify where resources can be best used to deliver timely and high-quality services
- responding to new and emerging issues by assessing the resources, skills, and equipment requirements for capability gaps
- prioritising the need for incremental investment by linking projects to the resources required to maintain capabilities and the resources required to mature capability
- embedding a capability lifecycle approach within internal planning processes
- identifying common issues and developing a more coordinated approach across capabilities to realise better outcomes, in terms of value for money and strategic public value.

Victoria Police noted that its capability development team has approximately 25 members, with representation from both operators (generally late-career police officers) and civilians with skills in strategic thinking, policy development, research and analysis, proposal writing, or some combination thereof. Victoria Police made a deliberate decision to build an internal capability development function, rather than seek external service providers. Victoria Police made this decision to maintain stability and knowledge within the capability development area.

U.S. Department of Homeland Security

Staff within the JRC support its mission to build a cross-DHS collaborative environment to validate and prioritise operational requirements for all major acquisitions, and to ensure that objective, analytical rigour supports those requirements. As a centralising and coordinating entity that supports capability development, this represents an example of the roles and functions Home Affairs might need to support capability development. The JRC has the following five missions:[10]

- implement and execute the JRIMS process, which includes coordinating document submissions
- review key documents to assess their quality, categorise them, provide analysis and coordination to support adjudication by council members, and validate recommendations
- train component staff on the requirements process, particularly in terms of providing standardised and authoritative training on the JRIMS process
- analyse joint capabilities and requirements through (1) the Capability Gap Assessment (CGA), which assesses capability gaps from across DHS in order to create a prioritised list of unmet capabilities for the department; (2) the Joint Assessment

[10] Michael Vasseur, Dwayne M. Butler, Brandon Crosby, Benjamin N. Harris, and Christopher Scott Adams, *An Assessment of the Joint Requirements Council's (JRC) Organization and Staffing*, Santa Monica, Calif.: RAND Corporation, RR-2473-DHS, 2018.

of Requirements (JAR), which assesses existing programs, in both development and sustainment, to create an investment decision support tool; and (3) a stakeholder working group that develops the approach and assessment criteria used by CGA and JAR[11]

- conduct requirements outreach, including advising various DHS agency requirements staff during the capability development process; and attending enterprise-wide forums related to requirements development, including acquisition review teams, policy development working groups, and DHS research and development integrated product teams.

Building the Home Affairs Capability Development Function

Having an endorsed approach to capability development represents only part of the solution. It is also required to have the internal capacity to support it.[12] All organisations that the RAND team reviewed have such a capability, often characterising it as an enabling capability (see Chapter Three). Further, the research team's interviews with officials from across the Department revealed that such a function is critical to the future success of Home Affairs, and that the function was currently lacking within the Department. While there will be a resource overhead on establishing this function (in addition to the resources required to design and develop the individual capability project proposals), best practices indicate that Home Affairs should establish a dedicated capability development function and provide resources accordingly.

It is implied in the development of the logic models for early phases of the CLMM that each model will require the performance of certain functions, which, in turn, assumes that to successfully execute the first four phases of the CLMM, Home Affairs staff will be required to develop specialised skills, knowledge and competencies. However, our analysis will examine frameworks that are employed by similar organisations to provide an overview of functions that Home Affairs could perform for each of the first four phases of the CLMM. Table 6.1 provides the outcome of the analysis. It shows that the necessary knowledge and skills within and between each phase of the CLMM are quite diverse and likely to require more capability development staff within Home

[11] As part of its continuous improvement process, the JRC has since replaced the CGA and elements of the JAR with a Capability Gap Register.

[12] This report does not examine the specific size, skill base, competencies or experience levels required for the capability development function within Home Affairs, as this is dependent on the structural and functional choices made within the Department, ABF and Portfolio. Factors include the governance model selected; the level of CLMM process complexity the Department chooses to employ; the nature, level of rigour and source of analytical support; the type of scrutiny that is applied; and the selected approach to accessing human capital.

Affairs. However, as noted, the exact number and nature of these staff will depend on implementation decisions made within the Department, ABF, and Portfolio.

Table 6.1
Capability Development Competencies

	Strategic Planning	Capability Requirements	Capability Definition	Investment Approval
Outputs	Capability Needs	10-Year Capability Plan	5-Year Investment Program	Capability Acquisition
Functions	• Provide policy and implementation support to the CLMM • Establish an evidence base for capability needs • Develop and maintain the strategy-to-capability mapping • Develop and maintain the vision of future operating environments • Ensure that strategic objectives, operational objectives, and operational tasks and functions retain their relevance • Develop and deliver decision briefs	• Provide policy and implementation support to the CLMM • Establish an evidence base for the capability plan • Assess the impact of program and project interdependency and interoperability • Establish capability value chains and associated roadmaps • Determine and prioritising capability gaps • Establish and maintain a capability risk register • Oversee the development of tier-two strategies • Maintain the 10-year capability plan • Estimate whole-of-life resources beyond the investment program including lifecycle cost estimates • Coordinate BoI review and undertake trade-off analyses • Support disinvestment decisions • Manage the alignment with enabling capabilities • Monitor and report on capability gaps • Develop and deliver decision briefs • Allow contestability and assurance	• Provide policy and implementation support to the CLMM • Establish an evidence base for investment program • Assess the impact of program and project interdependency and interoperability • Maintain a capability risk register • Initiate projects and support the CM • Support project governance based on complexity • Support initial business case development • Develop and evaluate capability design options • Estimate whole-of-life resources required for capabilities required within a zero to 5-year window including lifecycle cost estimates beyond the 5-year window • Coordinate program prioritisation through cost-benefit analysis and trade-off analyses • Support external engagement (other departments and private sector) • Develop and deliver decision briefs • Allow contestability and assurance	• Provide policy and implementation support to the CLMM • Develop and evaluate capability project options • Assess the impact of program and project interdependency and interoperability • Maintain a capability risk register • Support the CM • Support project governance based on complexity • Support final business case development • Provide detailed estimates of whole-of-life resources for each capability including lifecycle costs • Develop and deliver decision briefs • Support external engagement (other departments and private sector) • Support transition to acquisition • Allow contestability and assurance

CHAPTER SEVEN

Summary and Way Forward

RAND Australia was engaged by the Department and ABF to review the capability development framework currently employed within the Department and make recommendations on ways in which this framework could be matured. The outcome is an auditable, transparent and evidence-based approach that is flexible enough to meet the needs both of the Department and ABF, as well as, potentially, the other agencies in the Portfolio. The research considered and critically evaluated the CLMM as a whole, and then formulated a detailed framework for the first four phases of the model (strategic planning, capability requirement, capability definition, and investment decision).

RAND Australia's approach was to review key policy documents and undertake semistructured interviews with senior staff within the Department and ABF as well as Defence and central agencies. However, it should be noted that SMEs from other agencies within the Portfolio were not available to meet with the team during the course of the analysis. RAND Australia also examined capability development frameworks employed by relevant Australian and international organisations in order to identify lessons and best practice.

This report identifies 12 key findings on the current approach to capability development within Home Affairs. These led to a defined set of eight design principles for the establishment and implementation of a CLMM, a detailed capability development framework, and the identification of three options for governance models to support a future Home Affairs CLMM. Based on the analysis conducted to establish best practice in Capability Development, the RAND team makes the following recommendations.

Recommendation 1: Employ the capability development framework described in Figure 3.1. This framework captures the essential activities required within a mature Home Affairs capability development system, namely the translation of government guidance into capabilities that deliver the required effects and outcomes in a cost-effective and sustainable manner (Chapter Three).

Recommendation 2: Use the eight overarching principles for capability development within Home Affairs that are identified within this report. These principles are strategic alignment, a systems perspective of capability, decisionmaking, investment prioritisation, governance, organisational culture, internal and external engagement, and core business focus (Chapter Three).

Recommendation 3: Adjust Home Affairs' current FIC model by adding industry and organisation to the current set of inputs (people training; facilities; information and systems; equipment and supplies; support; and laws, policies, procedures, and administration) and use the definitions outlined in the report (Chapter Three).

Recommendation 4: Treat key enabling functions as strategic resources, and explicitly incorporate investment decisions associated with these functions when establishing the integrated investment program. At a minimum, the key enablers that should be included are capability development; ICT; RD&I; HR; strategic budgeting; critical infrastructure and estate management; state and territory engagement; and international partnerships (Chapter Three).

Recommendation 5: Consider an organisational structure that aligns with the two major activities of the capability development phases of the CLMM: capability identification and capability design (Chapter Four).

Recommendation 6: Incorporate the capability development approach into Home Affairs' corporate planning cycle, develop a 10-year capability plan, develop a 5-year integrated investment program, and use these plans to support capability investment decisions (Chapter Four).

Recommendation 7: Employ the interim logic models for capability identification, to transition to the mature model in the future (Chapter Four).

Recommendation 8: Employ the logic models for capability design to develop robust, evidence-based acquisition business cases that are adapted to project complexity (Chapter Four).

Recommendation 9: Recognise the key role SMEs perform throughout the capability development process, and invest resources to ensure their ongoing availability to those responsible for the capability development function (Chapter Four).

Recommendation 10: Choose the governance model that best suits Home Affairs circumstances; establish the necessary knowledge, systems and organisational structures to support it; and empower and resource key stakeholders appropriately (Chapter Five).

Recommendation 11: Establish and resource a capability development function (Chapter Six).

Recommendation 12: Develop a detailed implementation plan for institutionalising capability development (Chapter Seven).

Taken together, these recommendations establish a basis for implementing the proposed capability development approach. Clearly, implementation is contingent on approval by the senior executive. Once the decisions associated with the capability development model are made, including the choice of governance model, actions can be taken to make the necessary structural changes. The development of the detailed implementation plan would need to be shaped by the strategy for applying this across the Department. Given that the proposed CLMM model represents a major change to how Home Affairs currently operates, we anticipate that a phased rollout would be

suitable to facilitate organisational learning and process improvement, while minimising disruptions.

APPENDIX A

Capability Framework and Development Terms of Reference

The Terms of Reference for Capability Framework and Development Review component of the Capability Review stated that the RAND study

> is to assess the suitability of existing arrangements (including but not limited to framework, policy, governance, accountabilities and resourcing) associated with planning and management of capability across all phases of the capability lifecycle, with a particular focus on the strategy and planning phase of the Capability Lifecycle Management Model (CLMM).
>
> Based on the assessment above and informed by the findings from the capability baseline review, the review is to identify any gaps and propose a future state operating model, including but not limited to proposed governance, framework, principles, methods, policies, procedure, costing, risk management and structure for the Department's capability development function as well as whole of life management of specified operational capabilities.
>
> With respect to the strategy and planning phase of the CLMM, the review is to identify a process involving the development and progression of capability options through the investment approval process leading to approval – either internally or by Government.
>
> Given long lead times associated with major capabilities, the review should specifically focus on positioning the Department and ABF to establish a long-term view of its future capability needs, potential gaps and anticipated investment.
>
> With respect to the framework, the review is to clearly identify the current Capability Owner for all capabilities and, given the cross-cutting relationships of many of the Department's capabilities, propose mapping and organisation of existing capability domains with the clear identification of an owner of each capability domain.

> This aspect should have regard to work done by the Department to date and take into account governance, structures and arrangements between the Department, ABF and portfolio agencies.
>
> The review should provide a detailed implementation plan, including options for any alignment of functional responsibilities or structure, governance and process arrangements that will support the Departmental and ABF implementing an end-to-end approach capability lifecycle management.[1]

[1] Australian Government, Department of Home Affairs, 2018, pp. 2–3.

APPENDIX B

Study Methodology

In this appendix, we provide an overview of the methods employed for data collection and analysis. The data that underpin our analysis are based on interviews with senior Department and ABF staff, interviews with relevant staff from other departments, interviews with people from similar organisations in the United Kingdom and United States, an initial review of existing and emerging Department, ABF and Portfolio strategies and policies, and related policies and supporting documentation from elsewhere in the Australian government, and in existing academic literature.[1]

B.1 Interviews

In preparation for the interviews, the interview team sought to gain an understanding of the role and function of the positions that interviewees represented.[2] The interviews followed a semistructured interview protocol, intended to guide the discussion to topics of interest. Most interviews were programmed for 30 minutes, however many extended beyond this time, based on the richness of the discussion. The interviews generally followed the following construct, noting that some aspects being investigated were not pertinent to all interviewees:

- Interviews commenced by situating the interviewees in relation to how this study fit within the broader Home Affairs program of reviews, and explaining that the basis of the study is to support the development of a CLMM suitable for employment across the Home Affairs Portfolio.
- Information was sought to capture the interviewees' understanding of capability, capability development, and capability management.

[1] See Table C.3 for breakdown of interviews.

[2] Note the emphasis on the role represented, and that a significant number of those interviewed from within the Department were acting in the role they were representing.

- Where the interviewees felt they were situated within a capability lifecycle, we structured the discussion to determine where they contributed to it (input), their direct involvement in the process, and what they received from it (output).
- The interviewees' perceptions of the current capability development management approach (strength, weakness, constraints and opportunities).
- Where appropriate, the team elicited examples of current practices and identified lessons.
- The team asked what the interviewees required of and expected from an effective CLMM.
- The team allowed for an open discussion of additional issues such as workforce development and training, as necessary.

For the interviews with entities external to the Home Affairs Portfolio, the approach was for a more open discussion about their perception of the Department (and its predecessor, DIBP). Questions focused on engagement, current practices, lessons identified from other departments' practices, and recommendations for what constitutes an effective and efficient CLMM for Home Affairs.

Each research team member took notes during the interviews and these notes have been transcribed, allowing team members to identify and resolve any discrepancies. The interview notes were reviewed to determine the maturity of the current CLMM, determine the key factors that would be required to implement an effective CLMM, analyse options for closing gaps in the system's current capacity, and determine the key attributes of the proposed CLMM.

It should be noted that, at the time of writing this report, only members of the Department and ABF were available for interviews.

B.2 Document Reviews

Capturing a comprehensive view from DIBP and Home Affairs capability lifecycle policy and strategy documents has, to date, proved difficult. The Portfolio continues to evolve, and as a result capability lifecycle strategy and policy development is immature. The level of maturity of the capability lifecycle strategy and policy development is to be expected, given the recent establishment of the Portfolio. The result is that we were initially restricted to strategy documents from the organisational entities that have come into the Portfolio as part of the Machinery of Government changes. We also reviewed existing (unapproved) internal documentation that had been developed within the Major Capability Division in 2016 and 2017 that explored an approach to CLMM for DIBP.

We also sought to incorporate emerging departmental policy. We note that the first high-level strategy document for the Portfolio was released on 13 July 2018 (during

our baselining activity),[3] which we have included in our analysis. The Review and Reinvestment Roadmap (R3) process provided some interim documentation, although this was also in the early draft stage. We reviewed policy documentation from other departments (particularly Defence) to provide a basis for comparative analysis. Finally, we sought a range of internal planning and committee documentation to provide additional qualitative and quantitative data points. This documentation included investment planning documents, business cases, and historic acquisition and operational expenditure documents.

B.3 Workshop

In order to test the feasibility of the model, a series of workshops were held with Department and ABF staff. These were based around previous capability projects and sought to utilise their collective experiences to determine whether the recommended model was fit for the purpose intended. Each workshop considered a capability project suggested by the Department and relevant to the expertise of the area. The approach was for these officials to step through the logic models for the first four phases of the CLMM. Workshop attendees were asked to situate their project within each phase and comment on if and how the proposed model would have improved the development and delivery of the capability if it had been in place when it was initiated. It was emphasised that the workshop was not intended to critique how the project was actually developed, but to understand how it could develop under the model proposed for capability design.

As this was a simple desktop exercise to assess feasibility, definitive opinions on the suitability of each model could not be made. Instead, we reached a consensus opinion for each logic model. It is noted that in some cases, workshop attendees were not able to comment on each phase, due to a lack of background information. The information was collected and minor adjustments to the model were made.

---

[3] See Australian Government, Department of Home Affairs, 2018a.

APPENDIX C

Baselining Capability Development in Home Affairs

In this appendix, we summarise the current CLMM framework as described by the Department. This information is derived from DIBP documentation and so represents the approach prior to the formation of Home Affairs. The descriptions provided in this appendix have been derived from key documents provided by the Department, the existing literature and interviews with Department and ABF officials. This provides a baseline understanding of the CLMM approach, from both a policy and practice perspective. It provides some of the key inputs on our finding on the practice of and our recommendations for the principles for Capability Development within the Department and ABF.

C.1 Extant Definition of Capability and Associated Fundamental Inputs

Capability

The Terms of Reference for this review stated that 'capability for the purposes of this review is defined as the capacity and intent to achieve and sustain a desired effect or output in order to meet one of more strategic objectives'.[1] Having reviewed definitions in similar organisations, we believe it adequately conveys the necessary 'ways-means-ends' description.

Fundamental Inputs to Capability

To assess the adequacy of the FIC supplied by the Department, the study team made a comparison with other FIC-like models in Australia, the United States and the United Kingdom (see Table C.1). We observed that the set used by the Department appears consistent with comparable FIC-like models, notwithstanding the fact that the Department does not have a FIC dedicated specifically to organisation (which is currently captured under support). Given the more complex organisational structure associated with the Portfolio, as well as the intent to focus efforts and avoid duplication, work

[1] Australian Government, Department of Home Affairs, 2018f, p. 2.

Table C.1.
Comparison of FIC Components

Australian DIBP[a]	Australian Defence[b]	Victoria Police[c]	UK MoD[d]	U.S. DoD[e]	U.S. DHS[f]
People	Personnel	People (including training)	Personnel	Personnel	People
Training	Collective Training		Training	Training and Education	Training
Facilities	Facilities	Infrastructure	Infrastructure	Facilities	Equipment and Systems
Information and Systems	–		Information	–	
Equipment and Supplies	Supplies	Equipment	Equipment	Materiel	
Support	Support		Logistics	–	–
Laws, Policies, Procedures and Administration	Command and Management	Processes	Doctrine and Concepts	Doctrine; Policy	Doctrine; Planning
–	Organisation		Organisation	Organisation	Organisation
–	Major Systems		–	–	–
Industry	Industry		–	–	–
–	–		–	Leadership	Leadership
					Exercises and Evaluations
		Technology			

[a] These are taken from a slide pack developed by the Strategic Business Engagement Section of DIBP in 2017.
[b] Australian Government, Department of Defence, 2012a, pp. 2–3.
[c] Victoria Police, 2016, p. 9.
[d] UK MoD employs the term 'lines of development' rather than FIC. See United Kingdom Government, Ministry of Defence, "Defence Lines of Development Analysis with MODAF," 2009.
[e] Note that the U.S. DoD treats Doctrine and Policy as separate inputs to capability. See Defense Acquisition University, "DOTmLPF-P Analysis," *Acquipedia*, undated-b.
[f] See U.S. Department of Homeland Security, *Developing Operational Requirements: A Guide to the Cost-Effective and Efficient Communication of Needs*, version 2.0, November 2008.

across agencies, and seek efficiencies, there is a clear need to incorporate a FIC element that considers this. Otherwise, the risk is that capabilities will be stovepiped into functional areas, a major concern of many interviewees. Because of this, we suggest that an organisation FIC is warranted, given the expansion from DIBP to Home Affairs. The organisation FIC would incorporate the structural elements within the Department and agencies of the Portfolio; the distribution of the workforce across each of these functional areas; and the overarching leadership, control and governance mechanisms that enable coordination across these areas. We recommend defining *organisation* as

'appropriate structures, personnel and balance of competencies to accomplish operational tasks and to ensure appropriate leadership, control and coordination'.

Given the previous definition of capability, it is clear that a 'capability' is more than a system or platform. Rather, it is 'provided by one or more systems, and is made up of the combined effect of multiple inputs.'[2] In Australia, these are referred to as FIC. The Department has previously developed their own FIC with the following definitions:

- **People:** the appropriately sized workforce that has the necessary skills to perform the required role.
- **Training:** the education and skills development programs which enable the workforce to acquire and maintain appropriate skills and competencies.
- **Facilities:** the supply, development, and maintenance of infrastructure required to effectively implement specific capabilities.
- **Information and systems:** the reference and support materiel essential for the delivery of capabilities.
- **Equipment and supplies:** the assets, hardware and materiel required to implement capabilities.
- **Support:** the operational and corporate services that underpin capabilities, such as finance and maintenance support.
- **Laws, policies, procedures and administration**: ensuring that a capability incorporates all levels of required documentation and guidance.[3]

To this set, the Department, like Defence, has added industry. While we do not currently have a formal definition, we have used a working one, based on the following, which is employed by Defence:[4]

- **Industry:** the capabilities of Australian industry and the capacity of Australian businesses to deliver not only operational and other capabilities, but the full spectrum of support functions.

---

2 Australian Government, Department of Defence, 2012a, p. 2.

3 We were unable to find an endorsed document with FIC definitions. These definitions came from Australian Government, Department of Immigration and Border Protection, *Capability Management*, unpublished presentation, 2017b.

4 Australian Government, Department of Defence, 2016b, p. 19.

C.2 Key Enablers

Key enablers are enterprise-level functions that support and contribute to the efficiency, effectiveness and sustainment of operational functions.[5] They differ from FIC elements in that key enablers are crosscutting and concurrently contribute to a number of functions and capabilities. Each should be treated as a strategic asset with its own enterprise-level plan and investment strategy that most effectively and efficiently invest the Department's finite resources into the right capabilities at the right time.[6] These would be key components of the Department and Portfolio strategies, and would need to be incorporated into the capability plan and integrated investment program to ensure they are properly accounted for when determining the resources required to achieve the ambitions of the portfolio. This is particularly important, as Home Affairs is seeking to enact a shared-services model that centralises such enabling capabilities.

We note that, within the Australian context, key enablers are recognised and considered within the capability lifecycle. For instance, Defence, in its *Simplified Business Model*, identified 14 enabling capabilities,[7] and in the 2016 *One Defence Business Model* identified six enablers, four 'direction setting and contestability' functions, and four controls.[8] Similarly, Victoria Police has identified ten enabling capabilities.[9] These are compared in Table C.2.

As the table shows, key enablers are particular to the operational environment. As such, Home Affairs should determine what are its key enablers. From our discussions with Department senior management, along with our understanding of the operational environment, we suggest the following set of enabling capabilities:

- **capability development:** the function by which Home Affairs establishes, analyses and promotes its case for capability investment from government
- **ICT:** the enterprise-level architecture and systems that underpin all Home Affairs capabilities
- **RD&I:** the overarching strategy that future-proofs the organisation, capitalises on new opportunities and mitigates emerging threats
- **HR:** the strategic personnel plan that delivers the quantity and quality of people necessary to meet organisational demands while adhering to corporate and legal responsibilities
- **strategic budgeting:** the capacity to develop budget forecasts that inform enterprise-level planning across all relevant time frames

---

5 It is important to note that key enablers and operational capabilities should be considered equally.

6 Australian Government, Department of Immigration and Border Protection, 2016, p. 2.

7 Australian Government, Department of Defence, undated-c, p. 3.

8 Australian Government, Department of Defence, 2016a, p. 168.

9 Victoria Police, 2016, p. 17.

Table C.2.
Comparison of Enabling Enablers

Australian Defence: *Simplified Business Model* (2012)	Australian Defence: *One Defence Business Model* (2016)	Victoria Police: Enabling Capabilities
strategy and policy	policy and strategy (d)	
S&T	S&T is defined as a defence capability	innovation
		forensic science
capability development	force design and joint capability authority (d)	
HR	HR (e)	people management
garrison and estate management	facilities and estate (e)	property management
security	security (e)	
materiel acquisition and sustainment	capability acquisition and sustainment is defined as a defence capability	
financial management and reporting	finance (c)	resource management
audit and controls	enterprise performance and risk (d)	governance and assurance
	internal audit (c)	
	inspectors general (c)	
	judge advocate (c)	
ICT	information management and ICT (e)	communication
		information management
training	health logistics, education and training (e)	
health		
logistics		
legal	legal (e)	
	military command (d)	
		intelligence
		partnership management

NOTE: For the *One Defence Business Model*, we denote (e) as enabler, (c) as control, and (d) as direction setting.

- **critical infrastructure and estate management**: the estates and physical infrastructure necessary to support the delivery of all functions across the enterprise
- **state and territory engagement:** the provision of national-level coordination across key Home Affairs domains, through strategic and operational relationships with domestic partners
- **international partnerships:** strategic collaborative arrangements with international peers to enhance the capabilities of Home Affairs and its regional partners and to be a conduit for its domestic partners to engage with international partners.

C.3 Baseline Capability Lifecycle Model

The Capability Review Terms of Reference stipulated that the Department and ABF will be employing a seven-step CLMM (Figure 2.1).[10] These were based upon a previous efforts by the DIBP to establish a CLMM. While the seven phases were endorsed by the DIBP Executive, the approach, as proposed, was not. As part of the development of the documentation around a CLMM, DIBP developed definitions for each phase as follows:[11]

- **Strategic planning**, the first stage, focuses on strategy and its role in informing and shaping capability development. It provides a view of the Department's present and future direction to inform forward planning of operational and capital investment.
- **Capability requirements** is the point at which high-level capability gaps are identified, and proposals are reviewed and prioritised for funding, either externally via an NPP or internally through the DCB.
- **Capability definition** encompasses the development of business cases to support prioritisation of proposals only seeking external funding.
- The **investment approval** stage involves the preparation of NPPs and associated Cabinet submissions. Funding associated with proposals is considered by government as part of the budget process.
- The **capability delivery** stage is focused upon acquisition and development of capability, with additional focus on the downstream in-service management (sustainment) and subsequent disposal, and documented in the postinvestment procedural instruction.

---

[10] Australian Government, Department of Home Affairs, 2018f, Annex B. We note that the documents provided have had minor variations on this, particularly with respect to the naming conventions for phase 6, capability operation and sustainment.

[11] These are taken from a slide pack developed by the Strategic Business Engagement Section (DIBP) in 2017.

- The **capability sustainment** stage covers the requirement for the capability owner to monitor the various enabling elements and perform continual needs and requirements analysis to ensure that the acquired capability remains strategically relevant and fit for purpose.
- The **capability disposal** stage provides for the planned withdrawal of a capability at the end of its useful life. This phase is significant, as early identification of the planned withdrawal date initiates action in the capability requirements stage to plan for a replacement or follow-on system.

C.4 Interviews with Subject-Matter Experts

Establishing a baseline understanding of capability design, development, acquisition and management across the Department and ABF is a critical first step in developing the capability framework for the CLMM. This was achieved through a combination of semistructured interviews, strategy and policy documents, and select Portfolio and project documentation. This included conducting 52 semistructured interviews with 74 SMEs.[12] Fifty-seven officials from within the Home Affairs Department and ABF were interviewed, with 22 of these at the First Assistant Secretary or Deputy Commissioner level or above, including those acting at that level at the time of the interviews (see Table C.3). In addition to these interviews, discussions were held with other government agencies that have a mature approach to capability lifecycle management (i.e., Defence, Department of Finance, PM&C and Victoria Police), and international experts from the United Kingdom and United States. We also undertook a review of relevant government policy documents and reviews.

To understand the perspectives of senior Department and ABF staff about the current state of and issues related to capability development, we reviewed the interview summaries. Limiting this to interviews where Department or ABF Senior Executive Staff (SES) (or equivalent) were present, the number of interviews included was reduced to 33.[13] Interviews were structured to allow for a thematic analysis of the responses. Nineteen key issues emerged, characterised as representative statements shown in the following tables. We note that we have categorised those issues raised in the interviews into three types: those raised *regularly* in the interviews—five in total (Table C.4); those that were raised in a *significant minority* of interviews—eight in total (Table C.5); and those raised in *a few* of the interviews—five in total (Table C.6). This last threshold was designed to ensure that a representative number of interviewees (at least four) raised the issue. The distinction between the three tables was used as a form

[12] The interviews were predominately conducted face-to-face, with three conducted over telephone.

[13] Some interviews had multiple SES present.

Table C.3
Subject-Matter Expert Interview Summary

Organisation	Number of Meetings	Number of People Interviewed
Home Affairs Department—Executive Group	6	11 (3 FAS+)
Home Affairs Department—Intelligence and Capability Group	11	12 (5 FAS+)
Home Affairs Department—Coordinators	3	5 (3 FAS+)
Home Affairs Department—Other	10	12 (10 FAS+)
ABF	5	7 (3 DC+)
Other Australian federal agencies and state governments	8	15
UK government	4	7
U.S. SMEs	6	6

NOTE: FAS+ = First Assistant Secretary or higher; DC+ = Deputy Commissioner and higher.

of 'weighting' for the significance of the issue from an organisational perspective. We note that the categorisation is not orthogonal, as there are overlaps between the issues.

Table C.4
Key Issues Raised with High Regularity by Home Affairs Interviewees

Issue	Summary
Lack of a long-term, enterprise-planning approach for capability planning and development	Many raised the issue that the Department lacked a long-term, rolling investment plan that captured all elements of the capability lifecycle. The current approach was described as 'piecemeal', driven by short-term budgetary pressures, and was thought to be unsustainable. Examples were provided of how current practices have led to inefficient use of resources, failure to meet capability needs, and interoperability and sustainability issues. Many suggested institutionalising a capability plan that provides the organisation with a sound understanding of emerging gaps and challenges, an enterprise perspective linked to strategic aims and outcomes, and an understanding of resource pressures. Many suggested there was a need to build this discipline into the organisation. A 10-year time horizon was mentioned most commonly, likely reflecting knowledge of the current practice employed in Defence. However, some noted the benefits of having an additional shorter-term (more detailed) view that provides financial certainty in the 3- to 5-year time frame. It was also suggested that such time frames are needed to be able to represent the return on investment (particularly for revenue raising). Finally, it was recommended that decisionmakers take a more strategic approach to contract management, infrastructure investment, and developing Department and ABF internal skills and competencies.
Lack of a suitable governance structure to support capability lifecycle management	The lack of suitable governance oversight for capability management was seen as a major shortfall in the current system. Examples given included failures to transition between phases effectively, investment committee decisions being ignored, approvals for projects with incomplete business cases, inconsistent understanding of the accountabilities and responsibilities of Senior Responsible Officers (SRO), delivery trumping accountability, and the imposition of the same governance overhead irrespective of the complexity of an acquisition decision. It was suggested that since the Department (and Portfolio) are more complex and fiscally challenged than the entities from which they were constructed, a more transparent governance and approval approach was necessary. Some noted that the current committee structure is inefficient, with a lack of clarity on their purpose, inconsistent execution, and comprising too many participants offering comment in areas they do not have expertise. It was suggested that an optimal governance process would ensure clear authority and responsibility for SES officers, allowing both a reduction of administrative and process complexity and more capacity for improved and prioritised longer-term investment. Other suggestions for governance included distinguishing program management from project management and setting appropriate standards, and focussing decisionmaking on program delivery, adjustment and investment. It was noted that the impact on resources and skill sets of any strengthening of the SRO roles needed to be considered.
Lack of a 'golden thread' of logic that links investment to strategy	The failure to link the strategic outcomes (as defined by government) to investment decisions was repeatedly raised as an issue of concern. It was suggested that the gap between strategy and capability requirements led, on occasion, to a 'leap of faith' straight to deploying solutions. There were suggestions that this exposed the Department to risks in the medium- to long-term. Examples were given of NPPs being developed and sent to government without a basis in the underlying strategic priorities of the organisation. Some suggested that taking a strategy-led approach provides a better medium for confidence-building between the Department and the government, as it would provide earlier exposure to the Department's needs and link these to government expectations. It was recommended that the Department could develop theme-based concept briefs to articulate the problem, state what success would look like, and utilise some form of weighted assessment on benefits to support decisions.

Organisational structure and culture tend to inhibit progress rather than enable it	The disconnect between policy, acquisition and operator staff was frequently mentioned as a major limitation on the capacity for the Department and ABF to deliver an effective capability development program. It was noted that with the creation of DIBP, there was a centralisation of services, largely through the movement of support staff out of ABF. While the centralised functions were expected to support operators, it was observed that the relationships between those who moved into those centralised functions and the operators they had previously supported directly had been lost, in part due to the high rate of turnover of staff. As a result, some operational areas have considered reconstituting some of these capabilities, bringing in outside expertise, and building the competencies they require. Many suggested that a codesign approach that formally brings together the three areas be employed. However, it was noted that the different operating models within the relevant organisational areas were not currently well aligned. It was noted that while there may be the ability to use or improve current processes, the underlying cultural challenges need to be addressed.
Lack of capacity and experience in capability development	There was a strong sentiment that fundamental challenges to the implementation of a capability lifecycle model were a low level of maturity of the system, and limited internal experience, capacity and skills to support capability development. Significantly, it was noted that this is not a single skill set; rather, that different skills are needed for each phase and this should be recognised when institutionalising capability lifecycle management. For instance, while ABF operator staff can provide subject-matter expertise in identifying gaps, it was shown that this does not translate to developing requirements, exploring options, and delivering capability through acquisition. This has manifested itself through the purchase of equipment that is neither interoperable nor sustainable. It was noted that the lack of a dedicated capability development function and the appropriate number of staff to meet the current and emerging needs were significant shortfalls. A ‘centre of excellence’ model was suggested by a number of interviewees, as it was not seen as feasible to build a large capability the way that Defence does. In this model, the centre would train other staff in capability development to build knowledge, experience and consistency. The Capability Planning and Development Branch was suggested such a centre’s natural home; however, evidence provided showed a current lack of capacity and resourcing to meet future needs, and a distinct imbalance between specialist contractors and permanent staff.

Table C.5
Issues Raised Regularly by Home Affairs Interviewees

Issue	Summary
Current funding model cannot deliver long-term capability needs	Many believed that the current funding model for capability cannot sustain the aspirations for the new Department. Capability development budgetary arrangements are problematic, as these tend to be year-to-year, creating additional administrative overhead and program uncertainty. It was suggested that the funding approach is not sufficiently agile to support the business model. Some suggested that program planning is constrained by the manner in which the Department plan its annual budgetary cycle. The current budgetary requirement to offset new investments was also considered to be unworkable. Further uncertainty is created with delays in releasing budgets prior to the start of the financial year. There is limited flexibility in managing funds between NPP and the DCB, an issue which is made worse when projects hold onto their capital budget underspend too long. This was thought to limit the capacity to effectively reinvest within the financial year. This also creates downstream pressures, as those resources need to be rebid as part of the following year's budget proposal, in effect placing more bids under the same resources cap. Further examples were provided of the Department's failure to fund sustainment, strategic investment (such as technology), and (necessary) systems redundancy, creating future capability risks.
Tendency to focus on immediate threats rather than positioning for future challenges and opportunities	Many interviewees noted that acquisition decisions tended to be tactical, not strategic, characterising this as an investment strategy that focused on maintaining and remediating existing systems, rather than being driven by strategy-defined requirements. It was suggested that this led to broader risks, such as integrating new capabilities into outdated ICT systems. Further, there was limited consideration of the future operating environment when making acquisition decisions. Many suggested the need to move from a short-term 'fixing immediate issues' mentality to focusing on operational risk and gap profile over the next ten years. Some characterised this perspective as having little benefit, since those interviewed were not able to predict future threats and issues. Others suggested it was a response to the need to focus on managing immediate pressures facing the Department and on the in-year management of the Department. Many suggested that this was exacerbated by a disconnect between the strategy and operational requirements. It was also suggested that, unlike other similar domains, technology innovation generally comes from the bottom up and evolves from an operator-identified gap, leading to engagement with vendors to find new technologies. It was suggested the Department would benefit from being able to articulate the opportunity cost of building for the future, compared with addressing current problems, although this required consideration over a longer period than is typically considered.

Issue	Summary
Need to tailor the capability lifecycle model to be a scalable, enterprise approach	A number of interviewees were well acquainted with the process Defence employs, and while they expressed positive views on it supporting capability development at the enterprise level, they noted that capability development in Home Affairs was quite different. Differences identified included that the typical time frame is considerably shorter, that the number of large projects was considerably smaller, that the expected operational availability of capabilities was considerably higher, and that the investment approach was less certain and shorter-term in focus. It was noted that the same governance approach was employed for all projects, regardless of complexity, leading to smaller projects being overgoverned and had too many reports and roadblocks. Interviewees provided examples of large and complex capability systems within the Portfolio presenting challenges, such as an underestimation of future needs for sustainment, lack of consideration of end-of-life, and problematic contract management. This was generally attributed to the Department having few such projects and thus being unable to build the competency, knowledge and experiences in the same way that Defence did. Many suggested the need for a tailored approach that was flexible enough to adjust to differing agency and Department needs and project complexity. Suggested design principles included that the capability lifecycle model be designed to give a clarity of purpose for the portfolio; that it provide a simpler, more efficient and easier-to-employ process; and that it have the capacity to demonstrate (externally and internally) the achievement of outcomes. However, the common starting point for interviewees was a 'hub-and-spoke' model, where an organisational entity managed the capability development aspects of the more complex projects, while smaller projects would be managed by the delivery agencies.
Lack of an effective prioritisation approach to support investment and divestment decisions	A number of interviewees cited the lack of an established and formalised enterprise-wide prioritisation approach as a major constraint for the Department. This was characterised as the lack of a system to prioritise across the varying demands, inconsistency in capability requirements, a tendency to focus at too low a level, a lack of capacity to articulate cost or benefit or return on investment in a meaningful manner, and a lack of data and underpinning analysis to inform judgements. Some noted that there was a need for formal mechanisms that included disinvestment as a standard consideration in prioritisation. Interviewees gave examples where there was a failure to disinvest from systems that could no longer be sustained, and where there was an unwillingness to halt existing acquisition projects that are not working or where circumstances have changed. It was noted that a multicriteria decision analysis approach was employed in the most recent cycle, although the advice provided suggested that the investment that emerged and was approved was not enacted. It was suggested that Home Affairs utilise a risk-based approach for developing, prioritising, and adapting to change, to enable a determination of where to disinvest, divest and (re)allocate resources. It was suggested that while the Department does not prioritise well, this could be rectified if strategy was used as a launch point for decisions, where high-level guiding principles are used to provide consistency, and where assessment criteria are standardised and understood. Some noted the importance of a data system to support this, and that this system should capture all relevant inputs to identify gaps as well as ways to fill them. It was suggested that such an evidence base would better position the Department to understand the risks when it makes choices around bringing in new capabilities and closing existing ones. Many emphasised the importance of senior management buy-in.

Issue	Summary
Difficulty in delivering effective quality assurance and contestability functions	Many interviewees noted the inability of the Department and ABF to perform ongoing, and potentially independent, reviews of projects and programs across the capability lifecycle. This was characterised as a lack of contestability in capability requirements and options, an inability to performance cost assurance, a failure to define capabilities to demonstrate benefit realisation, high-level committee approval for investment plans that lack sustainment funding, and metrics that are not aligned with organisational outcomes. It was noted that financial contestability does occur—that is, the cost component of 'cost-benefit'. It was suggested that a consistency in and adherence to a standard approach would assist, as would sensitivity analysis.
Failure to plan and resource capabilities beyond their acquisition	A number of interviewees noted that sustainment and disposal of capabilities were not considered when making decisions around capability acquisitions. Further, some noted the transition between phases, such as the closing-out of a project after acquisition, was poorly done, particularly when the project crossed organisational boundaries. Some suggested the root cause was that the need to maintain the high operational tempo had a detrimental impact on sustaining capability, giving examples of where this occurred. It was noted that large and complex capability systems within the portfolio have presented challenges, with an underestimation of future needs for sustainment, lack of consideration of end-of-life, and problematic contract management. Some suggested that while the Department sought to articulate capabilities in terms of FIC, in practice, there was a tendency to define capability in terms of 'widgets'. It was suggested that institutionalising a model such as the Defence net personal and operating costs (NPOC) and better use of the FIC could assist as such a model would provide greater clarity on true cost of ownership early in the capability lifecycle, particularly for high complexity projects or where there are significant independencies associated with a capability.
Failure to recognise key enablers as strategic assets that require investment	A number of interviewees indicated that the focus on operational capabilities had led to an underinvestment in enabling capabilities. They considered these enablers to be important strategic connectors. However, there was a need for the new Department to draw them together to overcome a tendency to operate in silos. Some suggested that since these were not considered strategic investments, that there was a tendency to fund them from operating funds. However, over time, 'efficiency dividends' have taken a disproportionate level of resources from these. Many cited the ICT infrastructure as an example. Others noted that for some of the biggest capabilities in the Department, people were the biggest asset, and so there was a need for strategic investment in staff training. It was suggested that enabling capability requirements should include S&T, international engagement, intelligence, and legal frameworks.
Inconsistent understanding of capability	A number of interviewees recognised that while the term 'capability' was frequently used within the Department, the understanding of the term was inconsistent. This included the FIC, even though for business cases funding was described in FIC terms. Some stated this was based on some areas taking a platform or equipment view, rather than a systems or capability view. This was considered to be problematic, given that in some areas people were the key element of capability. This limited the scope for capability options since in some cases, a focus on people, rather than platforms, might offer a better solution. Some noted that the narrow definition of capability led to a focus on acquisition and operation of capability, without considering sustainment, disposal and interoperability. It was suggested that this represented an immaturity in understanding in some areas, and that this shortcoming had improved over time. Some interviewees identified the challenge of such an approach, as some capabilities were not well understood in terms of impact, so it was difficult to understand investment and return on that investment. It was suggested that one avenue to pursue was for senior management to specify capabilities and recognise those that are core to the operation of the Department, those that support the programs, and those that are unique capabilities.

Table C.6
Issues Raised by a Small Number of Home Affairs Interviewees

Issue	Summary
Tendency for replacement, rather than exploring new options	Approximately a quarter of interviewees explicitly identified as an issue for the Department the tendency to replace existing capabilities with something similar, rather than exploring new options for delivering the same effect. It was noted this was often a consequence of a lack of forward planning. Interviewees thought that this limited flexibility in terms of shaping capability and testing options. It was suggested that capability development needed to look beyond technological solutions. It was noted that the operational focus and existing funding instruments (e.g., NPP) meant capability design was generally near-term focused, supporting quick turnaround and delivery, and was characterised as a system set up to deliver solutions rather than explore options and opportunities. It was suggested that the Department would benefit from a capacity to consider replacements versus the capacity to replenish existing systems; a rapid appreciation of the 'system-level' perspective, leading to a strengthened ability to make trade-offs; and mechanisms to accommodate different types of investments.
Need for more strategic engagement with central agencies and government	A small number of interviewees suggested that the relationship of the Department and ABF with the central agencies and the federal government could be strengthened through a rigorous and defensible approach to capability proposals. They also noted that this will require a level of discipline within the Portfolio in how it strategically engages. Some suggested that earlier engagement with the Department of Finance would be beneficial to ensure that Finance officials are aware of emerging issues earlier than was often the case. They noted that NPPs were not a good vehicle for enabling this. It was noted that the operational environment was too dynamic for the legislation system to keep up, which constrained the solution space. Some felt that while it was beneficial to engage central agencies early, there were institutional constraints given that the Department has a need to align its own internal decisions before reaching out.
Capability requirements are not understood in a structured manner	Approximately 20 percent of interviewees suggested that requirements were not currently managed in a structured way. It was suggested that the Department needed a mature business architecture that codifies needs and requirements in a consistent manner, including incorporating, as early as possible, FIC elements. It was suggested that a robust analytical approach to developing and understanding capability requirements would help the Department to overcome a lack of understanding of what was being delivered by the capabilities being acquired.
Need to engage industry early	A few interviewees (mainly in the delivery area) recommended that earlier engagement with industry was beneficial in exploring capability options. Interviewees gave examples showing that earlier engagement could assist in determining potential commercial off of the shelf (COTS) solutions. Beyond COTS, it was suggested that contractual arrangements would benefit from activities exploring industry capacity, particularly in cases where a significant part of a capability solution involved the provision of external service providers. It was noted that a limiting factor within the Department was the lack of a business perspective in skills training and in the delivery model.
Need to recognise agency-specific statutory constraints	A small number of interviewees noted that specific agency statutory arrangements needed to be considered if Portfolio agencies' budgets were considered within a broader prioritisation activity. It was suggested that working together did not necessarily result in interoperability or consolidation, as each agency has particular needs, context and legislative limitations on how it performs its function. This was seen as a potential constraint on innovation.

APPENDIX D

Capability Development Practices in the Australian Public Sector

D.1 The Australian Defence Approach

Defence has been singularly successful in establishing and effectively implementing an end-to-end approach to capability. It has been employing holistic capability development frameworks since the Tange Review in 1973.[1] Given the longevity and maturity of the Defence CLMM, the Defence approach to the capability development lifecycle should provide insights for Home Affairs, so that lessons can be learned and approaches adapted to suit the Department.

The Philosophical Underpinning

Defence has a long history of applying a strategy-led approach for the development of Defence capabilities, producing seven Defence White Papers and three Strategic Updates since 1976.[2] These sought to provide a 'framework for making and implementing defence policy' where 'broad strategic concepts were closely linked to major structural reforms'.[3] These papers have been used to define 'the government's broad strategic objectives and the capabilities needed for them to be achieved within fiscally responsible and realistic boundaries'.[4] Hugh White contends that this implies the underpinning logic of these papers and strategies to be defining national strategic objectives, describing how and where Defence is expected to contribute to the achievement of those objectives, prioritising the capabilities that are required to achieve them, and making capability choices that align strategy, capabilities and resources.[5]

---

1 Australian Government, Department of Defence, 2015, p. 13.

2 Brangwin et al., 2015.

3 Peter Edwards, "Defence White Papers After 40 Years," Australian Strategic Policy Institute, 9 March 2016.

4 Brangwin et al., 2015.

5 White, 2008.

Defence defines this process as capability development, which aims to 'develop and maintain the most operationally effective and cost-efficient mix of capabilities required to achieve [the g]overnment's strategic objectives'.[6] As such, it ensures that Defence takes a strategic perspective when developing capabilities. The capability lifecycle is the 'basis for Defence's strategy-led Capability Development process, beginning with the development of a simple statement of user need that is developed into a capability solution for acquisition, introduction into service, operation and sustainment. The life cycle is completed with disposal of the Capability System'.[7]

Given the complexity of the Defence enterprise and the capabilities that underpin it, the capability lifecycle requires a portfolio perspective that is forward-looking, maintains an appropriate balance across all capabilities within existing resource constraints, and, as necessary, is flexible to adapt to changes in strategic circumstances. Along with a White Paper (and associated annual updates), Defence establishes a 10-plus-year-long Defence Capability Plan (DCP). These documents establish links between strategic guidance and capability, improve long-term cost forecasts, make capability-requirements development more rigorous, and improve program and project management. It is noteworthy that an underlying assumption of the DCP is that there is an agreed financial provision.

In the *Defence Capability Development Manual*, Defence identifies 'key tenets' as the basis for its approach to capability development. These are

- **Discipline:** A disciplined approach that reflects the intent and robustness of the entire process.
- **Choice:** Government must be provided with genuine, discernible, and affordable capability options from which to make an investment decision.
- **Time:** Proposals must be put to Government in sufficient time to permit a considered decision to be made without a gap in the Australian Defence Forces capability.
- **Joint and whole-of-government:** Every proposal provided to Government must consider its relationships to and impact on the broader force structure and, where appropriate, whole-of-government requirements.
- **Collaboration and transparency:** Proposals are developed collaboratively across Defence, and where appropriate, other Government agencies. This is achieved through an understood and agreed path that engages the appropriate stakeholders at the right time and highlights risks and issues concerning capability proposals at the earliest opportunity. Such an approach ensures that all elements of the investment decision are considered and are visible to Government.

---

6 Australian Government, Department of Defense, 2012a, p. 5.

7 Australian Government, Department of Defense, 2012a, p. 4.

- **Executable and sustainable:** The capability options put to government must be able to deliver the agreed capability baseline, within scope, schedule, budget, and workforce allocations, and be able to be sustained within Defence's resource boundaries.
- **Security and diversity of supply:** Capability options must consider the sources of supply and support for the capability in credible contingencies.
- **Risk-managed:** Every proposal must ensure that Government is aware of the risk it accepts in making an investment decision. Risks must be actively identified, analysed, evaluated, treated, and monitored to ensure that Government has a defensible and sound evidence base to support decisionmaking and the allocation of resources.
- **Value for money:** Value for money is the core principle underpinning Australian Government procurement, and requires a comparative analysis of all relevant costs and benefits of each proposal throughout the capability life cycle (i.e., whole-of-life costing).
- **Documented decisions:** A documented decision trail must be developed and maintained so that future decisionmakers understand the decision, trade-offs, and agreements made to achieve the desired outcomes. It is also a critical element of accountability.[8]

Under the DCP model, defence capability is defined in terms of the integration of a set of fundamental inputs (see Table C.1). From a development perspective, these are broken up into capability projects, which are phased to allow for evolutionary development over time. Each phase is typically described as a set of options which are reviewed, approved and then funded by government. The DCP is not set in stone. In addition to occasional fundamental reviews, there is the need to adjust the plan annually, given changes in the strategic environment, changing economic circumstances, emerging and disruptive technologies, or delivery shortfalls in project and program delivery. As a result, annual reviews are performed that result in delays, fast-tracking or deferrals of agreed projects.

Evolution and Review

Following the *Defence Procurement Review 2003* (generally referred to as the Kinnaird Review)[9] and the *Defence Procurement and Sustainment Review* (generally referred to as the Mortimer Review),[10] the Australian government established and adapted a new

---

[8] Australian Government, Department of Defence, 2012a, p. 5.

[9] Australian Government, Department of the Prime Minister and Cabinet, *Defence Procurement Review 2003*, 15 August 2003.

[10] Australian Government, Department of Defence, *Going to the Next Level: The Report of the Defence Procurement and Sustainment Review*, 2008.

approach for capability development and acquisition that was centred around two centralised agencies (the Capability Development Group and Defence Materiel Organisation) with explicit responsibilities for the design, acquisition and management of capabilities throughout their lifecycle. This can be thought of as breaking the capability lifecycle into two distinct phases: the *needs phase*, which focuses on the strategy, capability requirements and investment decisions processes; and the *acquisition phase,* which focuses on acquisition, sustainment and disposal.[11] This aligns neatly with the breakdown of the model shown in Figure 4.1.

The Kinnaird Review established a two-pass process for government approval of DCP projects. First-pass approval focuses on capability gaps and broad (and diverse) options for addressing these. Importantly, off-the-shelf options, where they exist, are used as benchmarks within options analysis, particularly in terms of the military effects and schedule issues. Government approval results in the release of resources to further develop selected options, so between first and second pass approval fully-developed business cases with detailed costs are established. It is recognised that the capability development process is complex. Therefore, efforts are made to balance the need for a rigorous evidence base with something that is practical. As such, an outcome of the Mortimer Review was to tailor the two-pass approval process to suit the complexity of the capability. As such, 'simple' projects could have a combined first- and second-pass approval process, whereas high-risk or high-cost projects might require additional passes that support a more incremental decisionmaking process.

Notwithstanding this, the *First Principles Review* found that extant processes were complicated, slow and inefficient; there was uncertainty over accountabilities and responsibilities at senior levels; unnecessary escalation of issues to senior decisionmakers; and process and governance approaches created inefficiencies and unnecessary rework. [12] These led to significant project delays and follow-on effects to the DCP. As a result, Defence further evolved the capability framework, better tailoring it to reflect the level of risk and complexity associated with each project.[13] One important feature is the treatment of FIC, with 'projects now scoped to be inclusive of all of FIC rather than materiel, infrastructure and/or IT-centric'.[14] Therefore, the basic phases of strategy, capability requirements and definition, acquisition, operations, sustainment and disposal remain, and it is in effect the processes for traversing within and transitioning between those phases that has been adapted.

---

[11] Australian Government, Department of Defence, 2012a, p. 4.

[12] Australian Government, Department of Defence, 2015, p. 13.

[13] Australian Government, Department of Defence, *Capability Life Cycle Detailed Design: Executive Summary*, undated-a.

[14] Australian Government, Department of Defence, 2016d.

Project Complexity and Maturity Assessment

To assess the scale, complexity, and risks of projects, Defence has previously employed the ACAT (Acquisition CATegory) framework, categorised as follows:

- ACAT I: strategically significant acquisitions that have highly complex project, schedule management, or commercial arrangements, and significant technical, operating, or sustainment challenges
- ACAT II: strategically significant acquisitions that have significant project, schedule management, or commercial arrangements, and significant technical, operating, or sustainment challenges
- ACAT III: acquisitions that can be managed by traditional project and schedule management techniques and have moderate levels of technical difficulty, operating, support, and commercial arrangements
- ACAT IV: acquisitions that can be managed by traditional project and schedule management techniques and have low levels of technical difficulty, operating, support, and commercial arrangements.[15]

A Project Maturity Score for each option is also used to support decisionmaking. This quantifies the maturity of a project option by assessing and benchmarking it against ACAT-like criteria throughout the capability development and acquisition phases. During the capability development phase, these are

- **Schedule:** What confidence do we have in the schedule?
- **Cost:** What confidence do we have in the project cost estimate?
- **Requirement:** How well is the capability requirement defined and understood?
- Technical understanding: How well do we understand the solutions?
- **Technical difficulty:** What is the technical complexity in delivering the solution?
- **Commercial:** What confidence do we have that industry can deliver the solution?
- **Operations and support:** Is the effect on the operating and support environment understood and planned?[16]

Key Lessons from the First Principles Review

The *First Principles Review* was commissioned by government in August 2014 to ensure that Defence was fit for purpose and able to deliver against its strategy with the mini-

[15] The ACAT is assessed against six criteria, namely acquisition cost, project management complexity, schedule, technical difficulty, operation and support, and commercial. Australian Government, Department of Defence, *Defence Capability Plan: Public Version 2012*, 2012b, p. 7.

[16] Australian Government, Department of Defence, 2012b, p. 3.

mum resources necessary. In response to the review, Defence adapted how it undertook capability development. This included the following:[17]

- Establishing a new capability lifecycle model as the core Defence business process for all major Defence projects, including capability and enabling (estate, infrastructure and ICT) projects. Importantly, project proposals now use the new Smart Buyer risk assessment framework to inform decisions about tailored approval pathways.
- Including development of a shared understanding of risk through capability lifecycle. Defence worked closely with the central agencies, particularly the Department of Finance and PM&C, to develop this process.
- Transitioning to the Smart Buyer decisionmaking framework, thus enabling CMs and project teams to identify key project risks and to develop tailored project execution strategies. These tailored strategies form a central part of the business case as projects progress through approval points.
- Implementing a new business framework for CASG, defining how the group governs, organises and manages operations more efficiently and effectively across the capability lifecycle, with a focus on achieving Defence outcomes.
- Establishing centres of expertise within CASG, providing support to ensure the right people with the right skills are provided at the right time. This includes recruiting staff, managing careers, creating development opportunities, and allocating jobs. The centres of expertise are also responsible for CASG's policies, processes and procedures.
- Creating a range of processes and forums to ensure ongoing improvement in the capability lifecycle process, involving senior representation from the CMs and delivery groups. The primary objective is to develop, improve, standardise and rationalise governance across Defence in support of the capability lifecycle to achieve capability outcomes.

The Smart Buyer concept was used as the core of the new capability development framework implemented by Defence. Within the Defence construct, a Smart Buyer[18]

- achieves good outcomes for its customers
- will enable appropriate financial return for its suppliers
- undertakes the roles that government must perform, and effectively outsources other functions when that is the smart thing to do
- has the organisation, skills and suitable decision frameworks to make timely decisions on the optimum procurement, project management, and approvals strate-

[17] As identified in Australian Government, Department of Defence, 2017a.

[18] As cited in Australian Government, Department of Defence, 2017e.

gies for each acquisition or sustainment program, based on its critical risk features; it has the agility to refine those strategies as new information becomes available
- uses industry best practice tools and techniques to execute projects throughout the capability lifecycle through sustainment in a way that strikes the optimum balance between performance, time and cost.

D.2 Victoria Police Model

Victoria Police has begun using a capability-based planning approach to capability development, underpinned by a capability framework that considers the full lifecycle of a capability and situates this within the strategic objectives of the organisation.[19] This is part of a longer-term plan by Victoria Police to position itself to adapt to the changing environment within which it must work.[20]

The Victoria Police approach was the result of an inquiry into the operation of Victoria Police, which found that while it was responsive to the threat of the day, it did not have a clear plan for meeting short-, medium- and long-term objectives in a structured and efficient manner.[21] The Victoria Police Blue Paper noted that 'the history of Victoria Police shows the danger of being swept along by waves of social and technological change, and responding only under external pressure'.[22] A shift in thinking was necessary as the Victoria Police determined that its focus needed to shift 'further towards prevention, as compared to enforcement, … to respond to the complexity of Victorian society, promote sustainable, long-term public safety, and tackle crime before it happens'.[23] Victoria Police established this strategic direction through their Blue Paper (a strategic document much like a Defence White Paper) which recognised that success required a combination of 'better matching of resources to demand by rethinking the traditional operating model, and improving capability through workforce reform and technology; and collaborating more closely through partnerships'.[24]

Recognising the need for flexible and adaptive service delivery in the face of external pressures and unexpected challenges, Victoria Police elected to take a capability-centric approach.[25] From this, it sought a mechanism that effectively related risk and

---

[19] Victoria Police, 2016.

[20] Victoria Police, 2014, p. 7.

[21] State Government of Victoria State Services Authority, *Inquiry into the Command, Management and Functions of the Senior Structure of Victoria Police*, 2011.

[22] Victoria Police, 2014, p. 7.

[23] Victoria Police, 2014, p. 26.

[24] Victoria Police, 2014, p. 23.

[25] Victoria Police, 2016, p. 4.

uncertainty, capability definition and its development, and resource management in a manner that allows for informed and transparent decisionmaking. Under its model, Victoria Police sought to use capability planning to understand where capabilities are in their lifecycle, design and choose between capabilities particularly in response to new and emerging threats, understand the interdependency between capabilities, and establish a structured planning process that allow for effective investment prioritisation.[26]

The initial step in this approach was the capability plan, which sought to provide a roadmap for achieving the 2025 organisational vision established in the Blue Paper by articulating the key objectives, the service delivery functions, and the underpinning (core and enabling) capabilities and the fundamental inputs that contribute to these.[27] The capability plan is explicitly embedded within the internal planning process, and consists of the following five elements:

- strategic and external drivers to situate the future operating environment
- capability framework to enable coordinated and planned actions to mature Victoria Police's capabilities over the next decade
- maturity assessment to help prioritise capability development and inform investment decisions
- capability plan to articulate the investments and organisational reforms required for capability development, delivery, and sustainment
- annual plan, which outlines planned actions and activities for development, delivery and sustainment priority capabilities.[28]

Through the capability plan, and within the capability framework, Victoria Police seeks to take employ a 'whole-of-life' approach that ensures that capability investment extends beyond the initial capability development and acquisition phase, and into sustainment. It defines the characteristics of the capability lifecycle to be the following:

- a strong focus on integration;
- planning and managing capability maturity;
- equal focus on developing and sustaining capabilities;
- understanding alignments between capability needs and demand forecasting, evaluation and review;
- focusing on embedding change through change management principles;
- creating an environment that encourages innovation and continuous improvement;

[26] Victoria Police, 2016, p. 5.

[27] Victoria Police, 2016, p. 8.

[28] Victoria Police, 2016, p. 13.

- understanding the performance of capabilities through establishing baselines and use of maturity measures;
- identifying and maximising opportunities to streamline internal processes;
- aligning strategy, business planning and policy; and
- aligning financial planning, procurement, portfolio management and risk models.[29]

Victoria Police defines 'capability' as 'what Victoria Police does, not where, why or how something is done,' with characteristics that are 'representative of stable business functions, [are] unique and independent from each other, [and represent] independent of processes, organisation structure, and assets'.[30] Explicitly using the FIC construct to define how a capability is acquired and sustained, it identifies five FIC—processes, infrastructure, people, equipment, and technology—though the authors note that the people component also includes training, capacity, and knowledge and skills.[31] Victoria Police has identified 18 capabilities categories (and then 78 subcategories) which it separated into eight core and ten enabling capabilities (see Table D.1).[32] There is broad alignment between these capabilities and those required by Home Affairs, particularly for enabling capabilities. However, we would observe that the Victoria Police capability set is very large and likely to be difficult to manage, compare and optimise. We would anticipate a smaller set of Home Affairs capabilities would be beneficial.

Victoria Police has worked through the capability framework, culminating in the delivery of an annual plan.[33] Its assessment is that this framework has enabled it

> to better assess and understand the maturity of all our organisational capabilities. It has also provided the focus to justify investments and reforms by demonstrating how each project contributes to building capability and the confidence of government and the community in our ability to manage our resources. Embedding the Capability Plan has realised benefits including:
>
> - Establishing common language for business planning and decisionmaking.
> - Facilitating greater alignment of plans and strategies across the whole organisation.
> - Removing siloes and duplication of projects and processes.

---

29 Victoria Police, 2016, p. 15.

30 Victoria Police, 2016, p. 10.

31 Victoria Police, 2016, p. 9.

32 Victoria Police, 2016, p. 17.

33 Victoria Police, *Victoria Police Capability Plan 2016–2025: Annual Plan 2018–2019*, State of Victoria, Australia, July 2018.

- Facilitating common understanding of business direction and priorities across various levels of the organisation.[34]

This provides capability requirements (defined as actions) for each of its seven primary tasks (or focus areas), against each of the capability areas, as well as assigning responsibility for those requirements. These are then brought together via a 'transformation pathway', which aligns all requirements across time.[35]

---

[34] Victoria Police, 2018, p. 12.

[35] Victoria Police, 2018, p. 22.

Table D.1
Victoria Police Capabilities

	Capability Category	Capability Subcategory
Core Capabilities	Prevention	Police presence and visibility; target hardening; early intervention
	Response	Managing demand; first responder and incident attendance
	Incident Management	Public order management; public event management; emergency management; crisis management; critical incident management
	Victim Engagement	Victim support; victim involvement; harm minimisation
	Offence and Offender Management	Offence detection; offence investigation; offender processing; witness support; offender management; offence pattern recognition
	Justice Procedure	Bail and remand management; custody management; compilation of brief; prosecutions; court order management
	Security and Protection	IPP/ VIP protection; government building security; critical infrastructure protection
	Regulatory Services	Probity checks; licensing; regulation
	People Management	Leadership development; workforce planning; occupational health and safety; training and professional development; people performance management; employee relations
	Resource Management	Financial management; procurement management; asset management; ICT systems
	Information Management	Plan and design; capture and secure; use; share; review, retain and dispose
Enabling Capabilities	Governance and Assurance	Policy development; strategic planning; portfolio and project management; internal audit; business performance; change management; risk management
	Forensic Science	Collection; analysis; interpretation; reporting
	Property Management	Collection; storage; disposal
	Partnership Management	Inter-agency collaboration; leveraging external expertise; cross-border liaison; stakeholder engagement
	Innovation	Environmental scanning; horizon scanning; research and development; service development; benefits management; knowledge transfer
	Intelligence	Collection; analysis and forecasting; surveillance; situational awareness; human source management
	Communication	Issue management; internal communication; external communication; community engagement

SOURCE: Based on Victoria Police, 2016, p. 17.

APPENDIX E

International Case Studies

This appendix provides additional details on the international case studies undertaken as part of this project. The first two sections present case studies from the U.S. DoD and DHS. The third section presents case studies from the United Kingdom.

E.1 U.S. Department of Defense

The U.S. DoD has extensive experience in capability development, albeit on a much larger scale and within a significantly different political, operational and fiscal environment from that of Home Affairs. This does limit the ability to make comparisons and identify lessons. We have, however, identified two areas that might provide useful insights, namely the use of the JCIDS process to fill capability gaps, and examples of how the DoD has sought to field operational capability through rapid acquisition approaches. As with the DHS examples described later in this appendix, one of these (JCIDS) represents a top-down, strategy-led approach, while the other (rapid acquisition) represents a bottom-up, operator-led approach.

Joint Capability Integration and Development System

JCIDS is a formal, deliberate process that aims to identify, assess, validate and prioritise the capabilities required to fulfil DoD's missions.[1] Upon identification of a capability gap, it seeks to resolve the shortfall by exploring combinations of materiel and nonmateriel (FIC) solutions (see Table C.1). Early in the capability design process, an analysis of alternatives (AoA) is performed. The AoA compares the effectiveness and cost of different alternative solutions that could fill a capability gap, and enables decisionmakers to select a preferred capability option. AoA comprises the following three key elements:

[1] Defense Acquisition University, "Program Management," Chapter 1 in *Defense Acquisition Guidebook*, Department of Defense, section 1-3.2.

- **Context:** this includes the capability gaps being addressed; the nature of the strategic risks; operational threats and operating environment; all underpinning assumptions, constraints, and limitations; and the time frame being considered.
- **Alternatives:** several alternatives are usually considered. The first alternative is generally the existing situation or system, and provides the baseline against which the other alternatives are compared. Each alternative is described, including its scope, its technical characteristics, when it could become operational, how it would be used, how it would be sustained during its service life, and any technical risks and technology maturity considerations.
- **Analyses:** this comprises a number of distinct approaches that provide differing perspectives on the problem. These include an effectiveness analysis, which determines how well the alternative would perform in filling the capability gaps; and a cost analysis, which estimates the total lifecycle cost of each alternative, including costs for development, production, operations and support, and disposal; which, in turn, leads to tradeoff analysis, whereby costs, effectiveness, and risks of all alternatives are compared.

Rapid Acquisition—Predator Unmanned Aerial Vehicle

The MQ-1 Predator was a UAV in service with the U.S. Air Force between 1993 and 2018. The Predator provided real-time ISR capabilities to tactical commanders and was later modified to carry out aerial strike missions using Hellfire missiles. It was privately developed by General Atomics Aeronautical System, Inc. (GA-ASI) to demonstrate that a UAV could remain aloft for more than 40 hours.[2] It was later bought by DoD in the late 1990s using a program to insert commercially developed technologies into DoD acquisition process in midstride.[3] After the terrorist attacks of September 11, 2001, demands for the Predator's capabilities outstripped its availability, and more Predators were bought using a series of urgent needs requests.[4] Ultimately, 320 aircraft were acquired at a cost of approximately $2.5 billion USD.[5]

The Predator was a highly successful program that followed an unconventional path from conception to deployment. The program never fully completed the formal DoD acquisition process. As noted above, high demand led to approval of multiple urgent needs requests from field commanders for the aircraft. Additionally, much of

---

[2] Richard Whittle, *Predator: The Secret Origins of the Drone Revolution,* New York: Henry Holt and Company, 2014, p. 28.

[3] This was known as the Advanced Concepts Technology Demonstrator (ACTD) program. See Thirtle, Johnson, and Birkler, 1997, pp. 11–17.

[4] Such requests were submitted by field commanders for systems they needed very quickly for ongoing operations. More than 25 requests were made in total for the Predator alone.

[5] Jonathan Wong, *Balancing Immediate and Long-Term Defense Investments*, dissertation, Santa Monica, Calif.: The Frederick S. Pardee RAND Graduate School, RGSD-378, 2016, p. 119.

its utility derived from creative, user-driven ideas that were pursued without explicit official sanction, and were later formalised. For example, its real-time video feed capability was originally 'hotwired' by an Air Force engineer using a commercial video compressor and a military satellite terminal.[6] GA-ASI acted on a verbal request from an Air Force general to add an aerial strike capability.[7] This approach resulted in some technical inconsistencies across the Predator fleet, but demonstrated the utility of a collaborative development approach that was centred on feedback from users in the field.

Key Insights

The Predator program provides several insights on how rapid acquisition and innovation can work, and what policies or practices an organisation could consider when establishing a rapid acquisition function. Key insights include the following:

- broad design guidance is best for rapidly developing new technologies
- multiple avenues give rapid acquisition needs the best chance to be supported
- focus should be on a limited number of goals to maintain speed in rapid acquisition
- rapid acquisition requires iteration to reach its full potential
- decisionmakers should plan to address eventual shortcomings.

Broad Design Guidance Is Best for Rapidly Developing New Technologies

The Predator's development benefited from an unusual corollary of the capability development process in the DoD. Typically, weapons systems are designed to fulfil a specific set of requirements. These requirements are often precisely specified standards (e.g., speed, endurance, capacity) that govern the design of a weapon and are developed from extensive modelling and simulation efforts, wargaming, and other analyses.[8] These processes in turn require a fixed set of notions about how the weapon system is meant to be used. The outcome is often a precise set of requirements that are difficult to modify once the design and development process for a weapons system has started.

Because the Predator was part of the ACTD program, its development proceeded differently. Rather than being tied to specific requirements, it fulfilled a broader operational need for a platform capable of providing 'continuous all-weather coverage of worldwide targets and intelligence information on mobile targets for the in-theatre commander that the current national, theatre, and tactical intelligence collection assets

---

6 Whittle, 2014, p. 98.

7 Whittle, 2014, pp. 189–192.

8 For a concise summary of this process, see U.S. Government Accountability Office, *Defense Acquisitions: DOD's Requirements Determination Process Has Not Been Effective in Prioritizing Joint Capabilities, report to the Committee on Armed Services, U.S. Senate*, Washington, D.C., GAO-08-1060, September 2008, pp. 4–6.

could not provide'.[9] This broader ACTD charter allowed the Predator program office to interpret its mandate liberally, test new and different approaches to solving technical problems, and invest in new capabilities that not only improved the Predator's reconnaissance capabilities but gave it new capabilities as well, such as an armed strike capability.

Multiple Avenues Give Rapid Acquisition Needs the Best Chance to be Supported

The Predator benefited from the variety of stakeholders and institutional processes that allowed its development to overcome obstacles and proceed rapidly. For instance, the Defense Advanced Research Projects Agency (DARPA) funded an earlier prototype of the Predator, called Amber, that allowed the contractor (Leading Systems, Inc., later acquired by General Atomics) to test range extension and energy-conservation technologies that were critical to Predator's endurance.[10] The U.S. Central Intelligence Agency (CIA) invested in a subsequent prototype, the Gnat-750, from General Atomics. The Gnat-750 was eventually deployed in the 1990s to the Balkans, where its operational concepts were developed and refined.[11] This eventually led to the ACTD program, which invested in the development of the final iteration of the technology, the Predator. These organisations had similar goals that drove them to invest in the programs that eventually culminated in the Predator. However, if any one of them were excluded from the Predator's evolution and development, the result would not have been possible. Similar organisational considerations will be true in any enterprise, especially when it comes to a potentially contentious process, like rapid acquisition, that cuts through existing practices. Allowing multiple paths to success, as was the case for the Predator, will help to ensure that ideas can be brought to fruition without being stymied by existing bureaucratic processes.

Focus on a Limited Number of Goals to Maintain Speed in Rapid Acquisition

Many DoD weapons systems are designed with economy in mind, in the face of the United States' wide range of security commitments. Systems are designed to be multifunctional and to work in many environments. However, the DoD's imperative to produce weapons systems that are 'jacks of all trades' often poses challenging problems for designers and engineers trying to create systems that can, for example, perform as well in the extreme heat of the desert as in the extreme cold of the Arctic. This is even more true when the system involves new and unproven concepts and technologies to the degree that the Predator did. However, the Predator's broad mandate allow its designers to reduce the engineering problem by deemphasising some qualities that would normally serve to make the Predator a general-use platform. The airframe is

---

[9] Lee Carr, Kristen Lambrecht, Scott Shaw, Greg Whittier, and Catherine Warner, *Unmanned Aerial Vehicle Operational Test and Evaluation Lessons Learned*, Institute for Defense Analyses, P-3821, December 2003, p. B-27.

[10] Whittle, 2014, pp. 57–59.

[11] Whittle, 2014, pp. 81–82.

more prone to weather effects, like icing, than typical aircraft.[12] Its ground communications link is not fully secure.[13] Trade-offs like these enabled designers to focus their problem-solving skills on characteristics more central to its mission (e.g., endurance). Other requirements were left for later development, or deemphasised generally.

Rapid Acquisition Requires Iteration to Reach Its Full Potential

The Predator program demonstrates the utility of an iterative approach to procurement. The basic airframe and camera set represented a small initial investment in an unproven technology. Had the Iraq and Afghanistan wars not happened, the Predator would likely have been procured in modest quantities and used sparingly for reconnaissance missions. However, post–9/11 operations showed that the Predator could be adapted to a wide variety of uses. Having only the barest technical requirements to adhere to, program officers, GA-ASI and end users were free to quickly implement modifications and improvements to take advantage of tactical opportunities.

An example of this iteration was the distribution of the Predator's video feed. Initial models of the Predator featured a video feed that could only be viewed—in real time—from the operator's booth. Intelligence analysts could be stationed with the operators to analyse the video footage, or they could view the feed from a recording. Over time, commanders (who often work in command posts, separate from the operator's booth) sought to get real-time feeds in their command posts to aid decisionmaking. Since the Predator's operator booths are often far removed from command posts, program engineers quickly developed a video compressor linked to existing Army satellite communications systems to allow commanders, even at the Pentagon, to view Predator video feeds in real time. This live feed was eventually extended to troops operating on the ground. In 2002, after initial American operations in Afghanistan, a U.S. Special Forces soldier approached General Atomics with a request to develop a capability for the troops on the ground—for them to be able to view real-time video feed. After two weeks of development, the ROVER system was developed, tested and sent to forces in the field. This sort of frequent iteration is often necessary for new, rapidly acquired technologies to develop their true potential.

Plan to Address Eventual Shortcomings

The key downside to such an unconventional approach is that the same freeform approach to design and implementation will eventually result in shortcomings if the program is successful and needs to be scaled up. Although rapid acquisition bypasses dealing with some issues like sustainability and training to maintain speed, those issues do not disappear; they will often become evident when a successful rapid acquisition program transitions into an enduring one.

---

[12] Whittle, 2014, pp. 107–108.

[13] Whittle, 2014, p. 220.

The Predator's roots outside of the conventional acquisition system left it less prepared to deal with its rapid expansion, particularly after 2001. Although the Predator was formalised into a program of record in 1998, it was overseen by the Air Force's rapid acquisition program office, which at the time specialised in customising small numbers of aircraft for highly sensitive (often classified) roles and missions. For a small program like the Predator (with only 56 aircraft in 2001), there was little harm in keeping the program in that office.

Keeping the program in the Air Force's rapid acquisition office allowed the Predator to rapidly and iteratively add capabilities to the platform. But the more informal environment in that office was not conducive to standardising processes or to fully and systematically exploring the Predator's capabilities or its long-term needs. For example, new capabilities were added to some Predators, but not to the entire fleet, resulting in an inventory of Predators with differing capabilities. This meant that the Predator never achieved design stability, which in turn prevented the Air Force from devising an effective sustainment plan. The ground control stations (GCS) built to fly the Predators also faced the same problem. At one point, there were 12 different GCS configurations, which led to higher sustainment costs and inefficiencies, and was sometimes dangerous for pilots who might be familiar with one configuration but not another. As the program began to scale up after 9/11, this became a serious concern.

By 2006, demand for the Predator reached a point where it was placed into the traditional DoD acquisition process, which was better equipped to scale up the program. There, the lack of a thoroughly developed sustainment plan, and overall contractor and program office inexperience with the traditional acquisition process, made management very difficult. The Predator program office had to expand the program and deal with oversight requirements that were not part of the rapid acquisition process. Once the program became a top-tier DoD program in 2009, the program office and GA-ASI had even more oversight tasks to deal with.

Additionally, the Predator's pathbreaking approach to its mission created a host of organisational challenges unrelated to acquisition. Although the Predator fulfilled an existing mission set (reconnaissance and eventually precision strike), its unmanned approach and the additional ad hoc capabilities were disruptive to the Air Force as an organisation. Who would fly the Predator? Was it distinctive enough to demand its own qualifications and create its own career paths? How should it be controlled and employed? Who had the authority to direct the Predator to fire at ground targets? The Predator's first-of-its-kind status and informal roots meant that many of these questions were not answered—or even asked—before the Predator was developed and deployed.

The Predator's roots as an ACTD left it unprepared for the rapid demand increase that took place after 2001. As operational needs increased, demands for more aircraft, more personnel, and longer flying hours for existing systems grew beyond the ability

of the rapid acquisition process to manage. These issues must be considered when a successful rapid acquisition project scales up.

Rapid Acquisition—Palantir Intelligence Analysis Software

The Palantir intelligence analysis software is a suite of tools that integrates over 30 different intelligence databases and provides an intuitive user interface. Palantir was developed privately by the founder of online payment platform PayPal, Peter Thiel, to spin off that company's fraud-detection technology into a more-focused product for intelligence analysis. Over $45 million USD in software licences for Palantir were sold to the U.S. Army, Navy, Marine Corps, Special Operations Command (SOCOM), and the CIA.[14] Palantir licences were largely purchased through rapid acquisition processes, though contract renewals were negotiated through conventional DoD contracting mechanisms.

Palantir's ongoing success stems largely from its greater focus on end-user requirements, compared with a similar program that was being developed in parallel. During Palantir's development phase in the mid–2000s, its designers listened carefully to the needs of intelligence analysts, who were, at the time, focused on identifying and targeting terrorist networks, particularly those in Iraq and Afghanistan. Designers drew upon raw intelligence databases that were most useful to analysts, and designed the user interface around how analysts executed their tasks. Palantir designers were focused on developing the optimal tool for the immediate needs of intelligence analysts.

In contrast, the Army was developing a roughly comparable software suite known as the Distributed Common Ground Sensor—Army (DCGS-A).[15] DCGS-A was designed for a wider range of intelligence tasks, going beyond analysing terrorist networks. It incorporated a larger set of raw intelligence databases and had more analytical functionality. However, these additional design requirements made DCGS-A more prone to crashes and glitches, and its user interface was difficult to use.

Palantir's approach eventually won over the DoD. The Navy, Marine Corps and SOCOM adopted Palantir soon after they were exposed to it. The Army was less welcoming at first; arguments between elements of the Army and between the Army and Congress about the merits of Palantir versus DCGS-A were heated and ended up in the courts, but the Army eventually relented and is integrating Palantir into its updated version of DCGS-A.[16]

---

[14] For a detailed case study on Palantir and rapid acquisition, see Wong, 2016, pp. 103–109.

[15] Ashlee Vance and Brad Stone, "Palantir, the War on Terror's Secret Weapon," *Bloomberg Businessweek,* 22 November 2011.

[16] Jen Judson, "The Army Turns to a Former Legal Opponent to Fix Its Intel Analysis System," *C4ISRNet*, 9 March 2018.

Key Insights

Palantir's development history offers generalisable lessons and insights for managing the rapid acquisition of new technologies and leveraging those outcomes to drive military innovation. The following key lessons are apparent:

- Rapid acquisition can enable different approaches to problem-solving.
- Rapid acquisition should be driven by user needs.
- Focus should be on a limited number of goals, to maintain speed.
- Rapid acquisition projects must be prepared to encounter bureaucratic resistance.
- Successful rapid acquisition brings its own challenges.

Rapid Acquisition Can Enable Different Approaches to Problem-Solving

The most striking aspect of the Palantir program was that its advocates used the rapid acquisition process to avoid the conventional DoD acquisition system and pursue a new approach to developing intelligence analysis software. The conventional acquisition process had already selected DCGS-A software vendors; DoD was not likely to reverse course. Because of the way technical requirements were established, Palantir's unorthodox approach to meeting intelligence software needs did not align with the conventional acquisition process. Palantir developers believed that the fundamental approach that the DoD was taking was incorrect. Palantir emphasised tight integration of a limited but commonly used set of raw intelligence databases. By focusing on this, rather than attempting to integrate a larger number of less useful databases, it achieved a level of functionality and software stability that DCGS-A could not match. Palantir could only test the approach by leveraging the rapid acquisition process to bypass the conventional acquisition system.

Rapid Acquisition Should Be Driven by User Needs

Palantir's solution was informed by close adherence to the needs of its end users. Software engineers were introduced to intelligence analysts early in the development process, at which point they elicited the analysts' needs and observed their tasks directly.[17] Early versions of the software were tested by analysts and feedback was collected and integrated. When the software was deployed to a new unit or organisation, Palantir engineers worked with analysts directly, to ensure that the software integrated seamlessly into the unit's intelligence analysis activities and that its users were trained to use Palantir. The focus on meeting user needs at all stages of development and sustainment enabled Palantir's success.

The need to focus on end-user needs is especially important when executing rapid acquisition. In DoD, rapid acquisition actions are initiated by end users. Their needs are often tied directly to an immediate problem that cannot be solved with existing tools or systems. By focusing on the immediate user's needs first, designers are better positioned to quickly deliver results. Rapid acquisition decisionmaking and the stake-

[17] Wong, 2016, p. 108.

holder engagement processes should be streamlined to prevent the process from slowing down.

Focus on a Limited Number of Goals to Maintain Speed

A corollary to the need to focus on user needs is that rapid acquisition organisations and the contractors supporting the effort must be willing to prioritise some design requirements over others to simplify engineering problems and to maintain speed. Palantir's focus on only integrating the most useful raw intelligence databases (which were already known, based on use history) kept software instability problems to a minimum without sacrificing utility. Normally, this kind of prioritisation would be discouraged by the strict performance, standardisation and functional requirements. These requirements are set by acquisition authorities to encourage a general-purpose product that would be useful for a long period of time, across a variety of operational contexts. Palantir avoided these restrictions by virtue of its commercial roots. DoD did not solicit a proposal or bid from Palantir; rather, Palantir's leadership saw an opportunity and capitalised on it with a combination of self-funding and strategic investment by the CIA's investment arm, In-Q-Tel.[18] This allowed the engineers, not the acquisition authorities, to determine the best approach.

Rapid Acquisition Projects Must Be Prepared to Encounter Bureaucratic Resistance

Military organisations pursue rapid acquisition to quickly fulfil capability needs that occur for these three reasons: the need was not previously considered by the acquisition authority, the acquisition authority decided that the need was not worth pursuing, or the need was identified by the acquisition authority but is not being fulfilled effectively.[19]

Using rapid acquisition for the latter two reasons often generates institutional resistance. In both cases, military organisations are using rapid acquisition to contradict or supplant the decisions of the established, conventional acquisition authority. This results in the resistance of acquisition authorities and stakeholders aligned with them to such attempts to undermine their bureaucratic position. Quite often, the only way to rectify such conflicts is through senior leadership getting involved.

This was the case for Palantir. It was fulfilling a need that DCGS-A was attempting to meet. Although it impressed Marine Corps and SOCOM acquisition authorities, Army leadership resisted Palantir because it felt that it was taking an incomplete approach to the problem. It was also deep into the process of developing DCGS-A; the other services had not proceeded with similar programs. Furthermore, the Army's resistance was exacerbated by Palantir's more relaxed organisational culture, which clashed with the Army's preferences. Although Palantir ultimately prevailed, it did so only after some very public conflicts with the Army that required congressional

[18] Wong, 2016, p. 104.

[19] Wong, 2016, pp. 31–32.

intervention and legal action.[20] Organisations pursuing rapid acquisition efforts should understand how their efforts may be negatively perceived by other stakeholders and should make efforts to mitigate those effects through engagement, compromise or appeals to higher authority.

Successful Rapid Acquisition Brings Its Own Challenges

Successful rapid acquisition efforts can sometimes result in the weapon or system being accepted as a permanent solution. In that circumstance, a range of considerations must be addressed to achieve a successful transition. The following are some of those considerations:

- **Generalisation:** Many rapid acquisition programs are developed to address immediate needs, and may need additional refinement before general use is possible.
- **Standardisation:** Many rapid acquisition programs are developed through iteration. Other programs contain variants to address specific needs. In this circumstance, platforms and systems need to be standardised for consistency.
- **Sustainment:** To save time when procuring systems, rapid acquisition processes typically do not account for sustainment and maintenance needs. Comprehensive planning after the fact will be necessary to ensure longevity of the system.
- **Training and personnel:** Personnel trained to operate rapidly acquired equipment and the training itself is often ad hoc. Training curricula must be developed and standardised. Changes to personnel assignments or qualifications may also be warranted.

Many of these factors are evident with Palantir. First, long-term sustainment may be difficult, because Palantir owns the code and raw data that is produced by the software, not the military.[21] Furthermore, Palantir's intense focus on developing a tool optimised for analysing terrorist networks needs to broaden to accommodate other more general intelligence functions, such as tracking information on peer and near-peer military threats. Lastly, although Palantir's interface is intuitive and easy to use, some training will be needed to introduce new analysts to the platform. As a rapid acquisition program matures, those organisations which will ultimate own the asset should address these considerations to successfully transition a rapid acquisition program into an enduring one.

---

[20] Judson, 2018.

[21] Ian J. Cruikshank, "Why The Army's New Palantir Contract Won't Fix Battlefield Intelligence," *Task & Purpose*, 8 August 2018.

E.2 U.S. Department of Homeland Security

As observed earlier, the U.S. DHS has a similar portfolio construct to Home Affairs and takes a similar capability-based approach to identifying, developing and employing systems of capabilities to meet government objectives. To explore this, we have used two case studies to tease out issues relevant to Home Affairs. The first is the JRC, which is representative of a strategy-driven, top-down, enterprise-wide, centralised approach which looks for increased efficiency and effectiveness through the consolidation of capability requirements across portfolio agencies. By contrast, the second case study, Minotaur, represents an example of a bottom-up, bespoke approach to the development and delivery of a capability driven by operator needs outside of the standard acquisition approach.

Joint Requirements Council

This short section summarises the key points including best practices and lessons from the JRC case and its relevance to Home Affairs. These are the following:

- Ensure top-level leadership support with a clear mandate.
- Establish a coherent strategy and clear objectives that are communicated to the relevant components.
- Develop specific, measurable, assignable, realistic, time-related (SMART) objectives and set clear implementation goals and timelines.
- Establish a communications strategy and include the strategy, tactics, objectives, and target audiences, as well as how success will be measured.
- Focus on a set of priorities that are clearly managed.
- Systematically seek inputs from the components, particularly for the operational expertise, and encourage them to take ownership where appropriate.
- Understand that a centralised approach to acquisition may not be appropriate for all acquisitions.

Background and Structure

The JRC was originally developed in 2003 and was charged with identifying crosscutting opportunities and common requirements among the DHS components to ensure that DHS used its investment resources wisely. Unfortunately, the 2003 iteration of the JRC was never fully implemented, due to a lack of senior management officials' involvement. The JRC was officially dissolved by DHS in 2006. However, in 2008, the GAO recommended that DHS reinstate the JRC to review and approve acquisition requirements and assess potential duplication of efforts. After eight years without an active effort to review requirements and prioritise investments across DHS components, the then–Secretary of Homeland Security, Jeh Johnson, directed the creation of a new JRC in June 2014.

The JRC was given a new start in April 2014, following a DHS guidance 'unity of effort' memo issued by Secretary Johnson. That memo directed the creation of a joint requirements process, led by a component-composed and component-chaired JRC. The stated purpose of the JRC was to validate and prioritise operational requirements—those capabilities that are necessary to conduct DHS's mission—for all major acquisitions, and to ensure that objective, analytical rigor supports these requirements. The JRC serves to identify opportunities for joint collaboration to enhance operational outcomes, effectiveness and efficiency across DHS.

The JRC consists of a chair and 14 members, called principals, who are senior executives or officers that represent key DHS headquarters offices and seven of the department's operational components.[22] JRC principals represent the views of both their components and DHS, and validate and prioritise capability needs and operational requirements. Among other responsibilities, the JRC is to provide requirements-related advice and validate key acquisition documentation to prioritise requirements and inform DHS investment decisions. JRC recommendations are intended to be supported by strong analytical rigor.[23] The JRC chair position rotates among the seven operational components to help ensure that the activities of the JRC are component-driven and to provide an operational focus to the JRC's work.

JRC Process

Figure E.1 shows the JRC and its components working together in the development of an implantation plan to respond to DHS strategy, and in the analysis, requirements generation, and validation phases. The JRC has four macro-level mission areas. The first mission is the implementation and execution of JRIMS, a process by which the department reviews and validates capability gaps and requirements to mitigate those gaps. The JRIMS process is the primary function of the JRC, and serves to review and validate component-level requirements. Components submit requirements documents for new capability gaps to the JRC for initial review, solicit comments from across DHS, and ultimately seek a validation recommendation from the JRC principals, who endorse and validate the document.[24]

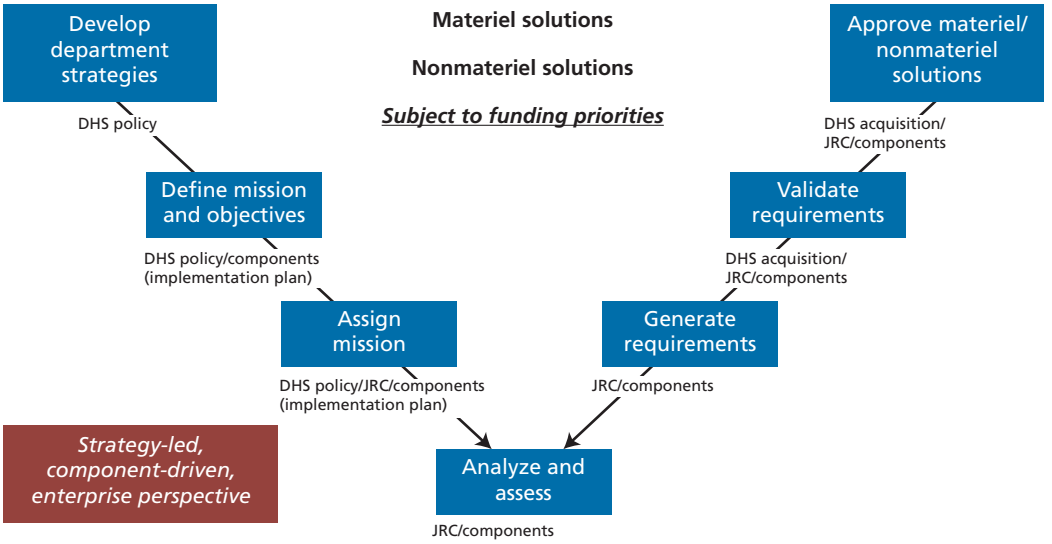
Figure E.1 displays the JRC approach to capability development and acquisition. It uses a two-step approach to capability development, namely to define the need (capability identification) and then analyse and select (capability design). Aside from outlining the types of activities and documentation that are developed, the process

[22] The seven departments are Customs and Border Protection, the Federal Emergency Management Agency, Immigration and Customs Enforcement, the U.S. Secret Service, the Transportation Security Administration, U.S. Coast Guard, and U.S. Citizenship and Immigration Services.

[23] U.S. Government Accountability Office, 2018.

[24] U.S. Government Accountability Office, 2018.

Figure E.1
JRC Process



SOURCE: Department of Homeland Security, JRC program office.
NOTE: The offices listed under the steps in the process are those tasked with that particular step.

also suggests that these two components represent a use structure for organising the capability development support function.

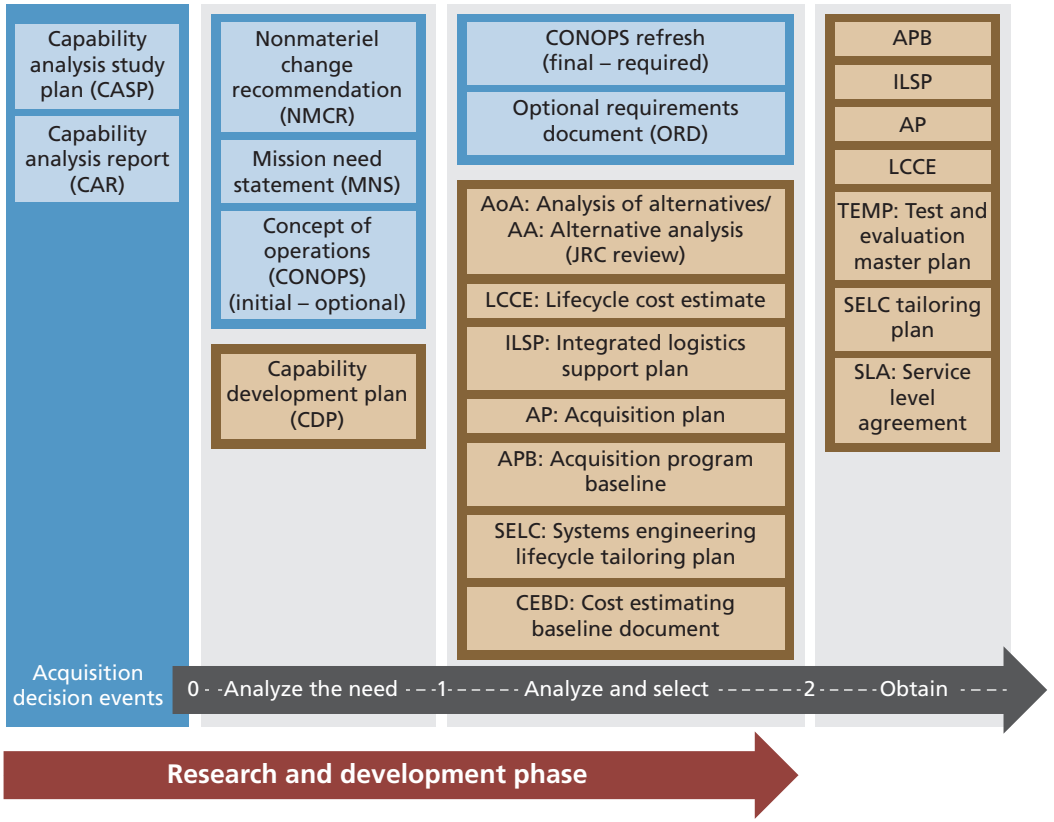
The second mission for JRC is the provision of requirements training to DHS staff on the requirements process. Figure E.2 shows the acquisition lifestyle framework currently used by DHS, which focuses on the acquisition decision events listed at the bottom of the graphic. The JRC is responsible for providing requirements training across DHS, but is primarily focused on the JRIMS process. The JRC is also responsible for the development and administration of a certification process for staff who receive requirements training. The delivery of this training is through multiday classes led by JRC staff.[25]

Third, the JRC is responsible for conducting analyses of joint capabilities and requirements, including assessing capabilities across DHS to create a prioritised list of gaps for the department and assessing existing programs to provide input to senior leaders on investment and funding decisions. Specifically, JRC oversees two efforts focusing on analysis of joint capabilities and requirements including the CGA, which creates a prioritised list of unmet capabilities for the department; and the JAR, which assesses existing programs, both in development and sustainment, to create an investment decision support tool.[26]

[25] Vasseur et al., 2018.

[26] The JRC has established the Capability Gap Register, which incorporates the CGA and part of the JAR.

Figure E.2
DHS Acquisition Lifecycle Framework



SOURCE: Department of Homeland Security JRC program office.
NOTE: Blue = JRC and JRIMS artifacts; brown = acquisition artifacts.

Fourth, the JRC engages in targeted outreach to various enterprise-wide forums related to requirements, as well as external engagements with entities outside of DHS. JRC staff offer various forms of support to components requirements staff during the development process, including informal review of documents prior to submission to JRIMS. According to the 2018 Homeland Security Operational Analysis Center (HSOAC) report, this mission area is challenging.

First, the JRC lacks the authoritative directives, policies and processes. Second, outreach efforts vary considerably among JRC staff, as each staff member works with different components, responds to different external requests, and participates in different committees or other meetings.[27] An interesting dimension to this task is the use of HSOAC SMEs to augment the JRC. Aside from offering their expertise to the components to assist in the requirements-generating phases, the additional 'value' of using

[27] Vasseur et al., 2018, p. 10.

outside staff is the neutrality that they bring, according to current JRC leadership. They are generally seen as trusted and respected partners in the process.

Separate from the JRC, DHS's Office of Program Accountability and Risk Management, which reports to the undersecretary for management, oversees major acquisitions and guides acquisition policy. DHS has a separate office for budget management and a planning, programming, budgeting and execution process to allocate resources, such as funding, to acquisition programs. The Science and Technology Directorate also conducts systems engineering reviews and technology assessments of the technical solutions for major acquisition programs. In addition to validation by the JRC, the undersecretary for management approves the operational requirements that the components developed and reviews them at a series of predetermined acquisition decision events. It is important to note that the JRC is largely outside of these acquisition processes within DHS.[28]

Since the JRC's renewal in 2014, it has engaged with senior leaders by briefing the Deputy's Management Action Group (DMAG) approximately every six months on the development of JRC's structure and processes, requesting approval from DMAG on the JRC's planned milestones and the composition of the JRC portfolio teams, and participating in Acquisition Review Board (ARB) meetings (see Figure E.3). DMAG's direction has provided the JRC with some of its short-term focus areas. For example, DMAG directed the JRC to focus on identifying commonalities between the systems used by components to screen and vet individuals for national security, immigration, and law enforcement purposes. The DMAG has supported the JRC by directing components to provide representation and part-time support to the portfolio teams. In addition, the JRC advises the ARB on capability gaps, needs and requirements that are the catalyst for investment decisions. According to one senior official, the new senior leader forums, specifically the Senior Leader Council and the DMAG, work well. They both foster transparency between the headquarters and the components.[29]

JRC's Outcomes

As mentioned above, the JRC has had a few starts and stops since its original inception in 2003. Since 2005, the GAO has made recommendations that DHS prioritise its major acquisition programs departmentwide and ensure that its acquisition portfolio is consistent with resource constraints. GAO has offered constructive feedback and recommendations to the JRC over the last 15 years. According to one DHS official close to these issues, a significant mistake was made early on, with the JRC leadership stating that it would now be 'component-led and component-driven'.[30] This statement, which caused conflict internally, ensured that for the time being the JRC would not

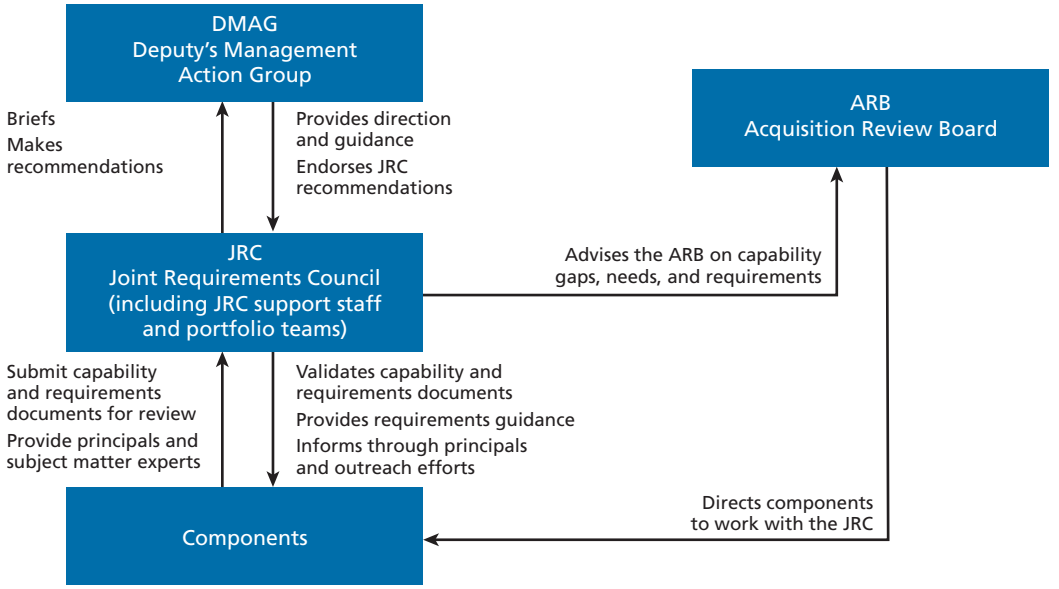
---

[28] U.S. Government Accountability Office, 2018.

[29] Discussion with DHS official, September 2018.

[30] Interview with DHS official, September 2018.

Figure E.3
JRC Internal Engagement Model



SOURCE: U.S. Government Accountability Office, *Homeland Security Acquisitions: Joint Requirements Council's Initial Approach Is Generally Sound and It Is Developing a Process to Inform Investment Priorities*, report to Congressional Requesters, Washington, D.C., GAO-17-171, October 2016b.

be directive, but could only make recommendations and provide advice. There is a tendency to not want to 'slow the components down'. However, one official remarked very directly that the requirements process is never going to work if no one is willing to say no. The other mistake was to task the JRC with reviewing the plethora of existing programs and then expecting the JRC to 'validate' those programs, rather than to consider their value to the department in the context of capability gaps. A third issue is that even though the JRC was set up to enable operator input into the acquisition process, the component members, including the portfolio leads, tend to have acquisition backgrounds. These communities think differently about risk: acquisitions SMEs tend to focus on cost, schedule and performance metrics, whereas operators focus on defeating the named threat. According to this official, the JRC and its portfolios need to have representation from the operations community, as originally conceived.[31]

In October 2016, GAO reported that the JRC's structure and management approach—informed by assessments of requirements processes, guidance and lessons learned from DHS components—are generally consistent with key practices for mergers and organisational transformations. However, they also recommended that DHS's Office of the Chief Information Officer have a more formal and consistent role than

[31] Telephone conversation with DHS official, September 2018.

that of a nonvoting advisor to the JRC, since 24 of 36 major acquisitions were information technology programs.[32]

In April 2017, GAO found that DHS's acquisition policy was not consistent with best practices for acquisition. According to this report, best practices call for ensuring that a program's needs are matched with available resources—such as technical and engineering knowledge, time and funding—prior to starting product development. GAO recommended that DHS require major acquisition programs' technical requirements be well defined, and that the department conduct key technical reviews prior to approving programs to initiate product development, in accordance with best practices. While this recommendation does not directly tie to the JRC, it does highlight a gap that JRC expertise could fill.[33]

One significant issue identified in 2018 by the GAO shows that nine of 14 programs from the seven components that were reviewed had changed key performance parameters for various reasons after program approval. DHS had initially approved most programs' key performance parameters before DHS reestablished the JRC in November 2014. Moreover, of all the seven DHS components, only the Coast Guard has a formalised policy in place for developing requirements. The others are in the process of developing a policy, or they simply rely on JRIMS. Here again, the lack of formal requirements processes across the DHS highlights the need for a JRC and for JRC expertise to support the components.[34]

JRC Process Insights

What Worked Well in the Program That Might Have Led to Successful Outcomes?

A former DHS official explained that one of the biggest challenges to the JRC is that the components do not understand its value. Some officials told us that there is value in having a headquarters organisation look at requirements holistically across all the components, whereas others consider the new JRC validation process to be an administrative burden and a waste of time. In any case, an emphasis on strategic communications from the leadership to the components and from the JRC to the components is needed.[35]

JRC officials have worked to build the organisation's reputation through an enhanced outreach program and strong analytic support. In its meetings with the components, there is a desire to be helpful and to 'keep it simple'. JRC staff (assisted by HSOAC) interact regularly with the components. JRC staff are based at the headquarters level, while the supporting external analytic support can be posted to the compo-

---

[32] U.S. Government Accountability Office, 2016.

[33] U.S. Government Accountability Office, 2018.

[34] U.S. Government Accountability Office, 2018.

[35] Multiple discussions with current and former DHS officials, August and September 2018.

nents on a temporary basis to advise on requirements products (in some cases, draft them, and in others, provide guidance). One such example of 'guiding' the requirements is that the surveyed analysts have pointed out the need to include cyber in the requirements. In part, the role of the analysts is to broaden the thinking of the components in the requirements space. Outside analysts provide the objective, SME-level support, and their neutrality is valued. In terms of accomplishments, there have been several noteworthy ones, such as the following:

- Prior versions of the JRC included only having a council with no support; the new version, from 2014, has corrected this deficiency with an enlarged staff.
- Since the components (with the exception of the Coast Guard) do not have robust requirements functions, a major role that the JRC has taken on is to ensure headquarters is aware of major acquisitions at the component level.
- In 2016, GAO identified that the DHS chief information officer (CIO) served as a nonvoting advisor to the JRC, even though most of DHS's major acquisition programs are information technology–related. GAO recommended a more formal role for the CIO, which DHS accepted.
- JRC has published a new 'user's guide' for JRIMS.
- JRC has created a knowledge-management decision-support tool, which tracks the capability and requirements documents as they are reviewed by stakeholders across DHS.

What Did Not Work Well That May Have Caused Unfavourable Outcomes?

DHS established its formal acquisition process in 2008, but did not have a similar emphasis on requirements development until 2016, when the JRIMS process was introduced. DHS requirements officials said that the renewed emphasis on requirements development at DHS requires a significant culture change among the components, pushing the components away from previous practices that undervalued well-defined requirements.[36] In the words of a senior DHS official, 'Good requirements set the stage to good acquisition. DHS needs a strategy-led, component-driven, enterprise perspective on its requirements and gapped capabilities'.[37] Without component-level requirements policies that are aligned with JRC and JRIMS standards, DHS is missing

[36] In 2016, GAO recommended that the DHS components develop an independent requirements generation process. Components need to ensure that requirements development is independent of acquisitions to guard against possible bias by acquisition officials toward a specific materiel solution. For example, if requirements developers were part of the acquisition function, management could tailor operational requirements to satisfy preferred acquisition outcomes, increasing the risk that capability gaps will not be addressed. The absence of an independent requirements organisation hampers the components' ability to remove biases and identify crosscutting opportunities and investments.

[37] Discussions with DHS officials, August and September 2018.

an opportunity to help ensure that components' programs are set up to meet end-user needs and close capability gaps from the beginning.[38]

A 2018 HSOAC report on the JRC found that it faces two major challenges: one in its organisational relationship to the DHS components, and one related to its staffing levels. Put slightly differently, the report talks about JRC's complexity and its relative newness as an organisation. The report summarises the complexity issues the JRC faces as follows:

- There are 14 operational and support component organisations within DHS. These organisations are led by high-ranking political appointees and federal career civilians. The roles and missions of some of these organisations do not overlap much with those of the JRC, thereby making it more difficult to integrate missions across organisations and execute the corresponding requirements.
- Conversely, some components have roles and missions similar to those of the JRC, thus requiring deliberate efforts to avoid redundancy and streamline requirements.
- Interdependence across the organisations results in a need for synchronisation.
- The wide range of requirements processes used by different organisations increases the challenge.
- The lack of budgetary authority, and a general organisational structure that places decisionmaking power in the hands of components rather than a centralised headquarters, serves to increase the complexity of the JRC's mission.[39]

As discussed above, the JRC faces significant challenges based on the nature of its relationship to the DHS components. JRC mission areas are based on a 'component-led and component-driven' requirements process, according to authoritative documentation and several interviews with JRC staff. As a result of the decentralised nature of requirements decisionmaking within DHS, JRC staff face considerable role uncertainty in their work. Many interview subjects expressed the idea that the only certain aspect of their work was uncertainty.[40]

GAO reported that JRC leadership considered lessons learned from the previous iteration of the JRC, which was established in 2003. For example, one lesson learned was that it is important to maintain departmental leadership focus on the JRC and continually engage with the components' representatives to obtain much-needed operational perspective. Further, for the new JRC to be successful, components need to see intrinsic value in the process so that they fully embrace it. However, one former DHS official explained to the RAND team that the JRC is largely disconnected from what

[38] U.S. Government Accountability Office, 2018.

[39] Vasseur et al., 2018, p. 3.

[40] Vasseur et al., 2018, p. 3.

the components are interested in, and the components are used to 'doing their own thing'. JRC was seen as disconnected from the requirements of DHS agencies and the realities of the acquisition process. The interesting acquisitions do not go to the JRC, and if there is only one component involved, the requirements also typically do not go through the JRC. In 2016, GAO found a very limited number of joint programs that had been validated by JRC.[41] JRC is 'floating' and not systematically connected to other DHS processes, including S&T. However, JRC is increasing its outreach efforts, in part to try and change the existing narrative, and promote the value of using JRC.

Vesting increased authority in the JRC over the requirements process would fall in line with best practices, and could improve JRC effectiveness and efficiency, in addition to any benefits provided to staff. The JRC currently lacks the authority to tie budgets to validated requirements, as well as the authority over existing programs, and receives most of its data from the component sponsor of a requirement. A JRC with more-robust authority over joint requirements, including over component actions, would improve JRC effectiveness, enhance JRC's ability to take an enterprise-wide view of requirements, and reduce the task uncertainty imposed on JRC staff.[42]

Related to its relative newness, the JRC faces significant staffing challenges across all mission areas. The report concludes that the JRC is understaffed given the current breadth of its responsibilities. This conclusion is based on evidence that staffing has increased as the JRIMS process demands have increased, but not at a pace required to fully meet all demands placed on the JRC staff. This tension is felt across mission areas: The JRC currently lacks one single full-time staff member dedicated to training, has limited analyst time for the analysis of joint capabilities and requirements, and requires the majority of its staff to balance the needs of keeping to the deadlines established in the JRIMS manual with their outreach responsibilities.[43]

Further, it is interesting that DHS officials have sought to learn lessons from the DoD Joint Requirements Oversight Council (JROC) on which the JRC is loosely based. DHS never intended to adopt the same process as DoD, because the two departments are fundamentally different. For example, DHS does not have combatant commands or a Joint Staff. DoD also tends to develop new systems, whereas DHS tends to acquire commercially available systems that meet its requirements. GAO also spoke with a retired JROC chair and a retired JROC member, both of whom shared the following lessons learned from their experiences that may be relevant to DHS:

- to be effective, the JRC must be a leadership priority

[41] The Maritime Patrol Aircraft Mission system was the only validated joint Operational Requirements Document.

[42] Vasseur et al., 2018, p. 3.

[43] Vasseur et al., 2018.

- DHS must understand the culture of its members and look for ways to break down barriers so that each entity is not operating in a silo
- having a quick process and cutting down on the length of the requirements documents is important; trying to capture too many details too quickly unnecessarily burdens the process and distracts from defining the capability gap
- DHS should not model the JRC after the JROC, because DoD and DHS are different and 'one size does not fit all'
- it is important to write requirements in a manner that can later be tested.[44]

Minotaur

Minotaur is a mission management system primarily used on surveillance aircraft by the U.S. DHS and DoD. These aircraft watch for vehicles and people on land and sea that could be involved in such suspicious activities as smuggling. Minotaur 'links sensors, cameras, radar and communications equipment into a single, more automated system, allowing operators to more efficiently identify and track any suspicious or illegal activity'.[45] It combines data from many sensors into a common picture, automates some functions such as moving sensors to focus on particular targets of interest, allows replay of sensor information, and tracks hundreds of potential targets at once.[46] That integrated information can be transmitted among aircraft and units in flight[47] and to operations centres.[48]

Minotaur provides an example of a capability, developed by one organisation, being adopted and integrated by other organisations. It was originally developed by the U.S. Navy,[49] and is now being used or tested on several platforms, including three Coast Guard surveillance aircraft,[50] four Customs and Border Protection manned and unmanned aircraft,[51] and two Navy aircraft.[52] The system is also reportedly being used by the U.S. Air Force.[53] Minotaur has been managed by the Navy and Customs and

---

44 U.S. Government Accountability Office, 2016.

45 Koscak, undated.

46 Koscak, undated.

47 U.S. Coast Guard, 2018.

48 Erwin, 2017.

49 U.S. Coast Guard, undated.

50 The three aircraft are the HC-130J Super Hercules, HC-144 Ocean Sentry and C-27J Spartan.

51 The four aircraft are the DHC-8, P-3 Orion, King Air 350 and the unmanned Predator.

52 The two are the P-8 maritime patrol aircraft and the EP-3E electronic reconnaissance aircraft.

53 Koscak, undated, and Richard Burgess, "Minotaur Mission System to Be Added to P-8 in Increment 3 Upgrade," *Seapower*, 5 April 2017.

Border Protection's AMO organisation since 2008.[54] The Navy, AMO and the Coast Guard cooperate on modifications to Minotaur.[55]

Minotaur is an open-architecture, government-owned system.[56] That means future updates will be easier, according to the Johns Hopkins University Applied Physics Laboratory, the software's developer.[57] Having multiple users means that costs for system updates can be shared,[58] and common maintenance, training and spare parts can help keep total costs lower.[59] Minotaur is now being provided as government-furnished equipment (GFE) for new platforms.[60] It provides data correlation and improved processing speed and memory over obsolete legacy systems[61] and, according to the Navy, has reduced operator workload such that one operator can do the work of three.[62]

Development and procurement of the Minotaur system intentionally took place outside of the standard DHS procurement system. Requirements for system enhancements are developed by the system operators and are implemented collaboratively by the user organisations.[63] System operators work side by side with the engineers developing the system, and there are no headquarters executive steering committees involved.[64]

Insights

Formal processes can achieve some benefits, but can also impose costs. Formal processes in areas such as requirements development and funding requests can have good intentions, such as a desire to get input from all potential stakeholders or to ensure that systems are designed to fill the needs of many users to improve efficiency. But those benefits can come with costs. Such processes can take many months to execute and may not always add value. A broad request to review requirements for a new system, for example, can result in comments and questions from offices that have no role in the operations being discussed and no experience with similar systems.

---

54 Erwin, 2017.

55 Discussion with DHS official, 29 August 2018, and Koscak, undated.

56 U.S. Coast Guard, undated.

57 Sharon Anderson, "Delivering Decisive Understanding to the Commander," *CHIPS*, April–June 2016.

58 "Innovative Tech Helps AMO Combat Smugglers."

59 U.S. Coast Guard, "Minotaur Mission System," webpage, undated.

60 Discussion with DHS official, 29 August 2018. GFE is equipment that is owned by the government and provided to a contractor for use on a government contract. See Office of the Undersecretary of Defense (Acquisitions, Technology, and Logistics), Acquisitions Resources Analysis, Property and Equipment Policy Office, "Frequently Asked Questions," webpage, undated.

61 U.S. Coast Guard, "Minotaur Mission System," webpage, undated.

62 Anderson, 2016, and U.S. Coast Guard, undated.

63 U.S. Coast Guard, undated; and discussion with DHS official, 29 August 2018.

64 Discussion with DHS official, 29 August 2018.

Less formal processes can also be imperfect. Such processes can sometimes depend on goodwill. The cooperative approach to managing and developing Minotaur seems to have been effective, and is enabled by the collaborative relationship between the AMO, Navy and Coast Guard officials overseeing the program.[65] It is possible that the program would fare less well if personnel turnover resulted in one or more officials who were less collaboratively inclined.

Close collaboration on requirements between system developers and operators is beneficial. Allowing the operators to drive the requirements and to work closely with developers to implement the changes has worked well for Minotaur, and has allowed its development to be very agile. A more formal, less adaptable approach would not likely have resulted in as good an outcome.[66]

E.3 UK Government

Cross-Government Capability Mapping

This case study describes the development and deployment of a new, cross-government approach to mapping capabilities to respond to and recover from civil emergencies in England and Wales. As part of the Resilience Capabilities Programme (RCP), the United Kingdom sought to employ a rigorous analytical approach to establish a capability map that provides a range of policy insights and supports tangible action to improve resilience. This was in response to the belief that government departments were assessing and developing capabilities in silos, independently of each other, and the lack of a common framework against which capabilities could be assessed.[67] The aim of the RCP, then, is 'to increase the capability to respond to and recover from civil emergencies', by improving government departmental understanding of the relationships between risk, consequence, and capabilities, so that the extent of preparedness is clearer and more accurate at a national level.[68] Unless otherwise stated, information in this case study was collected during an interview with representatives from the UK Cabinet Office on 1 August 2018.

The Capability Mapping Exercise

The capability mapping exercise is based on the UK National Risk Assessment, an annual process of identifying, characterising and comparing the major hazards and

---

[65] Discussion with DHS official, 29 August 2018.

[66] Discussion with DHS official, 29 August 2018.

[67] United Kingdom Government, Cabinet Office, 2018c.

[68] United Kingdom Government, Cabinet Office, "Guidance: Preparation and Planning for Emergencies," 30 May 2018b.

threats of national significance on a five-year horizon.[69] It is a multiagency process involving all government departments, as well as other stakeholders. The results are not public, but a public version is published.[70] The National Risk Assessment assigns responsibility for management of each identified risk to one government department. The assessed risks covered are grouped into three categories: natural events, major accidents, and malicious attacks.[71] The framework used for the capability mapping exercise, which is still being finalised at the time of the writing of this report, has three components, outlined in Figure E.4. The model has different capabilities for mitigation, response, and recovery (although it is expected that there will be many common capabilities). In relation to response, the RCP adopts a framework that interrogates response capability in seven capability elements, which, when taken together, represent a form of FIC.[72] These are further broken down into specific capabilities.[73] When the RCP started, there were no common definitions of response capabilities. These seven capability elements were selected by

- reviewing the National Risk Register and thinking in practical terms about what capabilities would actually be required to respond
- analysing historical events and the steps taken in response to those events
- consultation with government departments to gain endorsement.

Each capability is weighted in terms of its relevance to defined risks. For example, the capability to provide emergency shelter and sanitisation is highly relevant to the risk of a large-scale environmental disaster, but less relevant to an active shooter scenario.

The second part of the model is based on three assessment questions that aim to capture the rating of each capability, the evidence on which the rating is based, and the criticality of the capability. These three questions are asked about each capability, in relation to each of the risks to which that capability is relevant. It is noteworthy that one assessment question focuses on ensuring that information about the robustness of the assessment of each capability is incorporated into the model outputs.

The third element of the model generates an assessment of relative preparedness for each capability for each risk. There are four categories:[74] low confidence, midlevel confidence, high confidence, and more information needed.

---

69 Organisation for Economic Co-operation and Development, undated.

70 United Kingdom Government, Cabinet Office, "Guidance Risk Assessment: How the Risk of Emergencies in the UK is Assessed," webpage, 20 February 2013.

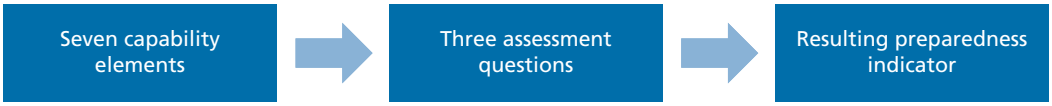
71 Organisation for Economic Co-operation and Development, undated.

72 United Kingdom Government, Cabinet Office, 2018e.

73 This more detailed level was not shared with the research team.

74 United Kingdom Government, Cabinet Office, 2018e.

Figure E.4
RCP Mapping and Assessment Framework



In summary, the RCP framework is designed to facilitate a self-assessment by every government department, for each capability the department is responsible for, in relation to each of the risks that those capabilities are linked to. As part of the development of the framework, the Cabinet Office conducted a structured interview with each department, during which each department was presented with and invited to comment on the definitions of the capabilities for which that department is responsible. They were then presented with and invited to comment on the list of risks to which those capabilities are relevant (to confirm that all the risks owned by that department have been identified). Following this structured interview, the department completed the self-assessment for all of the capabilities for which it is responsible (in relation to the risks those capabilities are relevant to), and reported data back to the Cabinet Office.

Outputs from the Capability Mapping Exercise

The outputs and impacts of the capability mapping exercise can be divided into the mapping itself and the knowledge and awareness generated as a result of the process of completing capability mapping. The framework is used to produce 'sunburst diagrams' that show the preparedness for each risk, based on the rating of the relevant capabilities.[75] These diagrams use 'RAG' ratings (red, amber and green, with purple representing a lack of information, and grey meaning workstream is yet to be assessed). They illustrate how the mapping of individual capabilities feed into a risk-level assessment of preparedness.

Different risk-level assessments can be visualised together in order to identify the risks where the most work is needed to increase preparedness, and the capabilities that drive the greatest preparedness gaps, capabilities that are used the most, and the interconnections between the capabilities. This visualisation creates the possibility of 'quick wins' through identifying capabilities that are critical to a number of risks or work streams, and thus where improvement could drive a number of benefits in a cost-efficient way.

As well as leading to the creation of the first robust, whole-of-government capability mapping exercise using a common framework, the Cabinet Office has reported that the process of developing the framework has also led to impacts. The structured interview process in particular, where the Cabinet Office met with each government

[75] See Data Visualization Catalogue, "Sunburst Diagram," webpage, undated.

department, was reported to have resulted in 'policy reflection, challenging assumptions, [and] enhancing understanding' among capability owners.[76]

Next Steps for the RCP

At the time of writing, the capability mapping exercise is being completed. It has taken around nine months, and has one full-time member of staff in the Cabinet Office (covered as part of business as usual costs) working on it. Going forward, the Cabinet Office has secured funding for the development of a software platform where each department or ministry can log in and update its capability mapping. Currently, the National Risk Assessment is only being completed at the national level—this means it is 'quite high level'. Some of the capabilities are owned and managed locally; there are plans to extend the exercise and use the framework at the local level, both to complete local-level mapping and to improve the accuracy of the national-level mapping. As yet, there is no evidence that the capability mapping exercise has led to shared capability development such as cross-government procurement, acquisition, training, or others.

Program Outcomes

It was essential that the capability mapping exercise was accompanied by a strong socialisation element. Government departments are subject to resource and time pressures, and some had initial reservations about the new framework. The Cabinet Office identified the following learning points to secure buy-in from the departments to engage in the exercise and participate in and complete the mapping:

- Departments' engagement was said to be secured by showing the new framework would not take any more time than their current risk and capability-planning activities (and in fact, would be quicker).
- Champions were identified in the departments who promoted the exercise.
- Many months were invested in face-to-face meetings with each of the departments, to explain the framework and its potential benefits.
- The national and wider international security context may also have motivated buy-in; all government departments are aware of the high likelihood of terrorist attacks in the United Kingdom. Additionally, domestic events, such as a fire in a tower block in London, meant that capability responsibilities and disaster response were in the forefront of many civil servants' minds.

Summary of Lessons Observed

This case study describes an example of successfully developing a common framework for capability mapping and completing a mapping exercise that puts that framework

[76] United Kingdom Government, Cabinet Office, 2018c.

into practice. It has resulted in an output which is usable by policymakers. Potential promising practices and lessons include the following:

- The model incorporates common definitions of capabilities and takes a risk-based approach. This means it can be used across government and is threat-agnostic. This approach was taken after the original approach experienced problems: the assessment was initially structured around planning assumption (i.e. predicted, common *consequences* of the risks listed in the National Risk Assessment) rather than the risks themselves. An initial pilot was based on this methodology, but found that stakeholders continuously drifted away from the planning assumptions and referred back to the National Risk Assessment risks when making their assessments. In response, the risk-based approach was adopted.
- The model integrates assessment of the evidence base that underpins capability mapping. This is a particular innovation of the framework. The evidence gaps are, therefore, clearly identified.
- The model uses a transparent, evidence-based, and systematic approach to arrive at the assessment, by using a common framework where elements of the framework are combined to arrive at overall assessments.
- The model can be deployed through a self-assessment approach, which is intended to ensure that the model can be mainstreamed and potentially used across local and national government
- The visualisation of the outputs of the model in sunburst diagrams makes them more user-friendly, so that the overall picture of capability can be easily understood.
- Championing the value of the exercise and stressing the efficiency savings for government departments if they adopted the approach was crucial to achieving buy-in and cooperation.
- Reassuring the stakeholders in government departments that the data collected would not be used for purposes other than for the risk assessment. There were concerns that the data would be passed to high-level officials, and could thus result in additional work, calls for explanations, or criticisms.

Strategic Planning Framework and Capabilities Model

This case study describes the development of a new SPF in the UKHO, part of which includes the development of a capabilities model. At the time of writing, the SPF and associated capabilities model are still in early stages (18 months into development) and are not yet embedded in the work of UKHO.[77] Both the SPF and the capabilities

[77] The model is not yet embedded across UKHO, while the final decision about if and how to use this more widely has not yet been taken.

model are to be treated confidentially. Information in this case study is drawn primarily from interviews conducted with UKHO officials.

The work to develop the SPF has been led by senior civil servants within the UKHO Strategy Directorate. The SPF is intended to address the following limitations with the current planning approach:

- There was a diversity of approaches across the different organisations and functions of the UKHO, in terms of quality of planning and strategies and the frameworks used for planning and forming strategy.
- There was some lack of coherence in terms of the long-term vision and objectives.
- Planning and strategies were short term (covering the next three years); identification of long-term trends and long-term planning were limited.
- Planning was largely bottom-up, rather than through a systems approach, working with wider partners, and identifying threat-agnostic capabilities.
- Strategies were constrained by geographic and institutional boundaries.

Specifically, in relation to capability, the problem statement included no common definition of capabilities; no complete picture of what the capabilities of the UKHO were; and no picture of common (or unique) capabilities, and thus limited understanding about where investment might have multiple beneficiaries.

SPF Development

The organisational environment in which the SPF is being developed is one where the responsibilities of the UKHO are shared between different (semi-independent) agencies and bodies, with their own budgets, cultures and capabilities. Responsibilities are shared locally, regionally and nationally (e.g., with elected mayors in some large cities, the National Crime Agency, local authorities, local police forces). This creates is a highly complex landscape and means many different kinds of stakeholders must feed into (and buy into) any strategic planning model.

The SPF is described as a framework for cross-sector use to link what the UKHO is trying to achieve with what it is actually doing across all partners and all activities. It is based around the interplay between ends (e.g., vision, goal, objectives) and means (e.g., missions, strategies, capability, financial plans) with influencers—mainly the internal and external context—and the FIC-like lines of development helping to moderate these. Importantly, the model uses a matrixed approach to distinguish the long-term, 10-year outlook (vision and mission) from the 5-year planning horizon (objectives, strategies and capabilities). Part of the framework is a 'capabilities' element, although this is in the early stages of development.

The program to develop the SPF was said to be based on strategic planning models outlined in the Open Group guide on Business Capabilities,[78] and on work

[78] The Open Group, *Open Group Guide: Business Capabilities*, G161, 2016.

done by the Business Architecture Guild.[79] These were described by interviewees as industry-standard models, providing approaches to translating strategy into delivery. Capabilities provide one aspect of that translation (along with others, such as how the organisation delivers value and how it links to technology).

The 'lines of development' in the framework are taken from these industry standards, which were used as a starting point, with some changes following a review of frameworks used across the government. Capabilities are not listed in the framework, but capabilities require a combination of all the 'lines of development' to be realised and implemented. At the time of writing, the capabilities had not been further defined. Further work is expected, specifically on the capabilities aspect of the model. The SPF was described as 'organisationally agnostic', indicating that it is intended to be relevant to the whole range of different organisations and bodies in the UKHO.

UKHO officials involved in the development of the SPF reported that a number of linked activities to develop the SPF, specifically around capability mapping, were completed. The team reviewed 15 departmental plans for 400 planned courses of action, set out in a range of strategy and planning documents.[80] The key findings about the quality and processes of strategic planning were that

- many courses of action were not clear
- there were commonalities between the strategies: For example, many mentioned early interventions that rely on data, communications, and working with others
- there was segmentation where similar approaches are undertaken in different parts of the organisation, which is not an efficient use of resources and confuses partners
- there were gaps: some goals did not have clear strategies, and there were gaps in implementation.[81]

The output from the review was a map of the different approaches to meeting goals, taken from different parts of the UKHO. The output also included identification of strategic goals and objectives that were and were not being implemented, gaps where goals and objectives had no corresponding actions, duplications, and common data requirements.

The next step was for broad consultation around vision and objectives. The group developing the model completed consultations with senior leaders from the different bodies and agencies within the UKHO about the vision and objectives for the UKHO

---

[79] Business Architecture Guild, *A Guide to the Business Architecture Body of Knowledge® (BIZBOK Guide)*, version 6.5, 2018.

[80] For example, large strategies such as the serious and organised crime strategy, counterterrorism strategy (CONTEST 3.0), as well as smaller strategies such as the tackling child exploitation action plan, modern slavery strategy, national border strategic assessment, drugs strategy, and so forth.

[81] Unpublished documentation provided by UKHO.

and its various parts. After these consultations, the team sought to identify the benefits of common capability planning. This was achieved through the production of a concept note that articulated and explored the potential benefits of approaching capabilities in a common way, and how this could be used to inform investment decisions and so forth. Finally, the team developed the draft SPF and began an initial mapping of calls for resources. When requests for resources were submitted by different bodies and agencies within the UKHO, these were mapped onto the draft SPF. This allowed the piloting of SPF, using it to identify duplication and commonalities (e.g., a border agency and a policing agency both plan to invest in identity-verification methods). This mapping exercise suggested the need to invest in common capability to get insights from data, for strategic engagement capability that manages collective requirements and priorities, and for a cross-sector analytical capability.

Program Insights

Given the early stages of development of the SPF, there have not yet been any outcomes in terms of joint procurement or planning across different parts of the UKHO. The implementation of the model has, to date, involved selected leaders in the UKHO agreeing to a vision, goals and objectives, and the piloting of the model in some parts of the organisation.[82] Those involved highlighted that the development of the model will be an ongoing process, as even once the model is in common usage, there will be future work to continually refine, update and adapt the model. More broadly, over the past four or five years, the term 'capabilities' has begun to be used, and a conversation has at least been started around capabilities and common capabilities. The following lessons relate to the progress made to date, and were described during the two interviews, namely:

- **Investment in engagement:** Time was spent on engagement with key representatives to explain the aim of SPF.
- **Broad consultation, as early as possible:** It was important to build relationships at the outset, especially among stakeholders in those bodies and agencies within the UKHO that have some independence in the way they operate.
- **Do not divert from core principles of planning and capability mapping:** It had been important not to allow significant adaptations to the model, and to insist, for example, that every capability must be linked to a business objective.
- **Linguistic differences might disguise a common capability:** This is common function for immigration and police forces, however, the language they used for this activity differed. Only after further investigating was it possible to determine that the ability to detain people was a common capability between departments.

[82] Interview at UKHO on 12 July 2018.

- **Focus on capabilities, not activities:** When parts of UKHO were asked about their capabilities, the tendency was to describe activities, which are different, and can lead to linguistic challenges and thus impede the identification of common capabilities.
- **Think about moving towards a capabilities approach, which raises fundamental questions:** The implications of an approach based on capabilities are potentially wide-ranging. This approach may raise questions about whether there should be changes to organisational structure (e.g., whether to restructure according to capabilities, rather than traditional areas of responsibility) and questions about whether UKHO is the right organisation to own or develop certain capabilities. While there was certainly no indication from interviewees that any significant reforms were planned, it had raised important questions about the ambition for this work to develop a SPF, how to employ it in the business, and where to take it next.
- **Difficulty in developing SMART objectives:** As part of the process of agreeing to vision and objectives, it had been challenging to ensure that all parts of UKHO articulated SMART objectives, and doing so had taken longer than expected.
- **Organisational culture and limited incentives to change:** Human factors and incentives were more important than the content of a common framework for capability, in terms of ensuring successful buy-in and implementation. The key is to shape an environment in which actors are motivated to participate in joint capability identification and definition.

Home Office Centre for Applied Science and Technology Commissioning Hub

This case study looks at the development of a Commissioning Hub within CAST in the UKHO. CAST 'provides expert advice, innovation and frontline support for the Home Office and its agencies on any issue relating to science and technology … [and] supports the full range of Home Office priorities in the areas of policing and tackling crime, counter terrorism, border security and controlling immigration'.[83] This case study is based on an interview with a senior official within CAST, conducted in September 2018.

Since April 2018, CAST has been integrated into the UK Defence Science and Technology Laboratory (Dstl—a group within the MoD), although its main focus is still on the science needs of the UKHO.[84] The aim of the integration was to 'improve the resilience of the science and technology support that makes such a major contribu-

[83] United Kingdom Government, Home Office, "Transparency Data: Senior Staff Salary and Structure Information for Home Office: March 2016," webpage, last updated 2 March 2018.

[84] United Kingdom Government, "Centre for Applied Science and Technology (CAST) Becomes Part of Dstl," webpage, 24 April 2018a.

tion to the nation's defence, policing, security and resilience'.[85] Dstl 'provide[s] sensitive and specialist science and technology research, advice and analysis for the UK Ministry of Defence (MOD) and wider Government… [and aims to] provide a more coherent and resilient capability for our customers'[86] by working with CAST.

Over the last two years, in the run-up to the integration and continuation after the 'official' integration date, a programme of work has begun to systematically assess S&T needs across UKHO, and to establish a commissioning process for new UKHO S&T needs,[87] referred to as a 'commissioning hub'. This is still in the early stages of development, so lessons are best thought of as potentially promising practice, and cannot yet be proven or independently verified.

Commissioning Hub

The Commissioning Hub has been created to understand user requirements for S&T across UKHO. The Hub has a mandate to commission work to address these needs from wherever best they can be delivered. Finally, it was stated that the Hub aims to exploit the benefits of S&T developments, 'looking for collaboration and cooperation where appropriate, both internal to the Home Office and across the Home Office and wider government'. A UK official noted that the aspiration behind the creation and ongoing development of the Hub is to understand how the relatively small budget available for UKHO S&T can be used to meet 'the most pressing and high priority Home Office needs'.

The Commissioning Hub has nine full-time staff (three account managers: one covers law enforcement; one covers borders, immigration and citizenship; and one covers homeland security) and a small team looking at business process, benefits analysis, and portfolio management. The Hub has access to four police advisors. Discussions indicated that these advisors have two roles: one looks at the identification of customer needs, while the other involves assessing whether the S&T research delivered is practical and useable by the police service.

In addition to the establishment of the Commissioning Hub, the UK government has established a UKHO Science and Technology Oversight Board, chaired by the UKHO chief scientific advisor. This board, for the first time, has visibility of all the S&T being conducted across UKHO. The board has already made some decisions and work has been commissioned as a result.

---

[85] United Kingdom Government, "Integrating the Science and Technology Support for the UK's Defence and Security," webpage, 24 January 2017.

[86] United Kingdom Government, *Defence Science and Technology Laboratory Annual Report and Accounts 2017 to 2018*, Defence Science and Technology Laboratory, 18 July 2018b, p. 9.

[87] United Kingdom Government, Home Office Science Advisory Council, "Minute of the Home Office Science Advisory Council," 28 September 2017.

Developing Capability Needs

Through the Commissioning Hub, the UKHO now has a consistent approach for capability needs, in a similar manner to the approach taken by the UK MoD. The instrument for this is the 'statement of user need', which seeks to articulate capability need, major risks and possible capability solutions. Given a lack of experience in the operator community for working in this space, the 'statement of user need' is established through the following four simple questions:

- What is the problem?
- What major risks are being addressed?
- What capabilities will be drawn upon in addressing the problem?
- How will the solution be exploited?

Armed with this statement, CAST and the Commissioning Hub make an assessment of whether and how S&T can be meaningfully applied in developing a capability solution. Whether science can address the problems identified is an important question, as users may have a tendency to focus on a materiel solution (e.g. supplies and equipment), assuming that a scientific or technological response is the best way to address the problem. However, nonmateriel approaches (e.g., a change of policy, an organisational change) may offer a more effective, more efficient and less expensive solution.

While outputs are not yet quantifiable in terms of efficiency savings from joint procurement, there was said to be strong progress towards a single procurement strategy, where many parts of the UKHO would be able to exploit the same piece of commissioned scientific or technological research. The CAST senior official interviewed for this case study reported that the use of the statement of user need had only been established for five months, but had resulted in the identification of common needs and, as a result, research completed for the police service was now being shared with the fire service and prison services. We also note that at the time of writing this initial needs assessment had been completed through a 'bottom-up' approach, looking at the existing work done by CAST. However, there were already some examples where senior-level user needs were being submitted to the Commissioning Hub.

Once all needs are considered and evaluated together, the Endorsed Science and Technology Programmes will be established as the basis for commissioning work. These are programmes of work, endorsed senior (director) levels in the UKHO.

Insights

The official who manages the creation of the Commissioning Hub advised that it was essential to secure buy-in and support from all parts of the UKHO. Support was forthcoming at the most senior levels, but at more junior levels, the need to change practice to move to a UKHO–wide approach was not obvious. This was often because there were examples of good practice in delivering S&T needs in some parts of the organisa-

tion. However, this resulted a range of different approaches for needs assessment, categorisation and commissioning. To support the different parts of the UKHO to better articulate their S&T needs, the Commissioning Hub undertook a series of workshops, to spread knowledge about the types of S&T available.

The approaches and new organisational structures are very new, so it is too early to determine their effectiveness. However, the senior responsible office in Dstl leading the changes reported the following factors as contributing to effectiveness, which therefore could be considered potentially promising practices:

- the creation of a dedicated team in the Commissioning Hub with a cross-organisation mandate to understand user needs that could be addressed by S&T
- the adoption of a standard framework for stating using needs
- securing senior-level buy-in, and placing the Commissioning Hub within an organisational structure where steering is provided by a UKHO–wide Oversight Board
- extensive work to explain the new framework and seek buy-in at junior levels
- leveraging instances where a common approach has brought benefits to further secure buy-in
- successes in the adoption of common approaches across different parts of the UKHO; examples identified during interviews with UK officials were
  - Forty-three different police forces in England and Wales had previously identified S&T needs separately, and tasked separately to address those needs. Now, as a result of CAST, forces coordinate their approach and it was reported that a Science and Technology Board for Policing had been established. This was described as a 'massive step forward' and unprecedented in UKHO. In future, it is hoped that similar boards could be created for other areas of UKHO responsibilities, such as borders and homeland security.
  - An oversight board has been established to look at S&T needs across all the directorates and parts of the UKHO.

While there had been progress, it was still the case that complete buy-in to the new approach had not yet been secured; there were still some parts of and functions within the UKHO that were not convinced of the need for a portfolio-wide approach. Interviewees indicated that support for joint approaches was strong at the most senior levels of the organisation, but this was not replicated throughout. Engagement and communication to secure buy-in to new approaches to needs assessment only went so far. Information provided suggested that in some parts of the organisation, change and adoption of the new approach only occurs when these steps to convince and persuade are complemented by a top-down mandate that all parts of the organisation must follow the new methods. Another area for development was to improve the identification and articulation of future needs beyond the next five years. Scientific and tech-

nological research can take several years to yield results, so research must be commissioned now to address future anticipated needs.

APPENDIX F

Observations from Baselining Activity

Based on the interviews and a review of key documents on the current state of capability lifecycle management within the Department and ABF (including opportunities and gaps), our key preliminary observations are as follows.

There is an appetite among the senior Department and ABF staff to change to a strategy-centred approach to capability development and acquisition that incorporates a whole-of-life perspective, rather than focusing on the acquisition and operations phases. Perspectives on how to make this a global change align with either single end-to-end oversight, or a distinct separation between capability development and acquisition. A holistic long-term capability planning program should be investigated as it could enable trade-offs, prioritisation of capability development proposals from one year to the next, and longer-term benefits realisation. This is manifesting itself in emerging documentation from the Department,[1] as well as other areas within the Portfolio.[2]

Robust capability development requirements need to be clearly linked to capturing operational needs and traceable to strategic objectives. It was a commonly held view that one legacy of DIBP in capability development was the gap between strategy and acquisition, and this legacy has manifested as a bottom-up approach to capability definition and acquisition. Internally and externally (domestic and internationally), it is recognised that there are clear benefits in ensuring a clear linkage between strategic guidance and acquisition strategies by establishing metrics that show clearer reporting between the operational and strategic levels, and by clearly defining standardised approaches to establish, prioritise and develop genuine options for realising the capability. Lacking a top-down approach driven by strategic priorities, some areas in Home Affairs are developing their own internal strategies and processes to manage their businesses.

There is tension between those who favour pursuing a threat-based approach to capability, which tends to invest in solutions to address immediate issues, and

1 Australian Government, Department of Home Affairs, 2018a.

2 Australian Federal Police, 2017.

those favouring a risk-based approach, which seeks to design capabilities to meet enduring challenges. It is clear from discussions with Home Affairs senior officials and a review of strategies that have been produced by different parts of the department and ABF,[3] and from internal investment planning documentation,[4] that there are differing perspectives on what constitutes capability and how capability should be developed, acquired and managed. From an enterprise perspective, this appears to revolve around a risk-based versus a defined threat-based approach to capability planning. This is not surprising in an organisation that is primarily operational, and which faces direct and sometimes rapidly evolving threats. This manifests itself, on the one hand, in a top-down approach that seeks to future-proof Australia by optimising protection against a broader range of threats and which conceptualises capability as a system comprising all the inputs to capability (FIC), and on the other hand, a bottom-up approach that seeks to react to threats by adapting existing platforms and structures. Both perspectives are appropriate; however, they should be acknowledged, and formal arrangements put in place to manage them (as departments such as Defence do).

Staff in Home Affairs appear to use risk- and threat-based language interchangeably. This leads to inconsistencies in capability development and acquisition strategies, as the latter tends to focus on procuring solutions to immediate problems.[5] We were advised that this interchangeable language and these processes have contributed to inefficiencies, as the systems being deployed are 'cobbled together' rather than properly architected as capabilities. It is recognised nationally and internationally that best practice is a risk-based approach, where capabilities are established based on a broader range of often not-well-defined threats.

Institutionalising a capability lifecycle approach across the Portfolio will take time, resources and commitment from senior management, as it entails changes to governance, organisational culture, processes, and training and development. Previous attempts to establish a capability lifecycle model in DIBP did not receive management endorsement. While the reasons are unclear, this experience does demonstrate that institutionalising this process successfully at the Department and Portfolio levels is a complex endeavour.

International experiences in the U.S. DHS have shown that concurrently integrating agencies into a new department, while seeking to develop a more-strategic approach to capability, requires a cultural shift both in terms of unity of purpose and establishing trust. This takes time and resources as staff, processes, systems and infor-

---

[3] See, for instance, Australian Government, Department of Home Affairs, 2018a; and Australian Government, Department of Immigration and Border Protection, *Strategy 2020*, 2015.

[4] For example, Australian Government, Department of Immigration and Border Protection, *2017–18 Five Year Investment Budget*, Capability Planning and Resources Committee: Agenda Item 3 Attachment F, 29 August 2017a.

[5] This has been an issue for Defence communities in the past (see De Spiegeleire, 2011, p. 21).

mation evolve and mature. Inconsistency in senior management has seen such entities as the DHS JRC make slow progress.

The UKHO is currently in the early stages of developing a portfolio-wide capability lifecycle management approach. Developing the model has been in process for around 18 months, and it has received considerable resources in terms of time invested by senior staff in the organisation. Even after this time and investment, however, interviewees from the UKHO indicated that the model was still in development, with the most challenging issues of ensuring buy-in and implementation still ahead.

Victoria Police took a number of years to develop, test, mature and institutionalise its capability development approach. They commenced in a single domain (forensics) and used lessons from that domain to develop and roll out an organisation-wide approach. They also did not seek to mature all aspects of the process at once; rather, they developed key components first to achieve (and demonstrate) improvement, and then built upon these achievements. Victoria Police have now completed three cycles of their capability development approach across all capability areas, and continue to modify and expand their model.

Similarly, Defence has continued to evolve and adapt its approach. It is noteworthy that the *First Principles Review* recommended a series of changes,[6] particularly in areas of governance and process.[7]

It is incumbent on Home Affairs to employ a robust and transparent process that incorporates all elements of the capability lifecycle, to give government the confidence it needs for capability investment approvals.

There is widespread concern that capabilities are not sustainable due to a lack of funding. This view reflected insufficient attention being paid to sustainment in funding proposals and (historically) in budget planning. While the internal Department budgeting system (Budgeting, Reporting and Costing System [BRACS]) now has made funding of sustainment explicit,[8] evidence shows that such funding was underutilised in the most recent budget-planning cycle. Many Department and ABF officials stated that lack of proper consideration of sustainment in capability planning was a key impediment to Home Affairs being able to deliver the expectations of the government.

The DCB process is used for funding new capability acquisitions below certain monetary thresholds. It is approved, through a competitive process, for a year-on-year basis, despite many of these capability systems requiring multiyear funding to meet contractual or other commitments.[9] NPPs are a primary capability development fund-

---

6 Australian Government, Department of Defence, 2015.

7 Australian Government, Department of Defence, 2017b.

8 See, for instance, Australian Government, Department of Home Affairs, "Factsheet: Capital Costing," internal document, undated.

9 Australian Government, Department of Immigration and Border Protection, 2016.

ing source for larger acquisitions. Collectively, these have led to some significant limitations for capability development, since they only cover the annual budget, with NPPs extending out to up to four years as part of the government's forward estimates. It was suggested that these drive a focus on acquisition and operations, as there is uncertainty over medium-term funding. Further, it was suggested that since NPPs generally require agencies to find financial offsets, there was a bias towards a replacement mentality as like-for-like replacement offers a simplified response. This results in a perverse outcome whereby 'new' policy proposals are more likely to steer away from exploring new capabilities.

There was a broad consensus that the budget reduction programmed in the forward estimates, and based on the efficiency dividend due to the formation of the Portfolio, is unlikely to provide Home Affairs with the resources it needs to support its strategic objectives in the short term. The initial data-collection activity conducted by R3 supports this observation. Examples were provided that demonstrated that the current budget is struggling to sustain the existing systems. It should be expected that an initial increase in funding is a necessary precondition to establish long-term efficiencies.

The quality of capability decisionmaking is currently constrained by Home Affairs' lack of maturity and consistency in policies, frameworks and language. Department staff are still trying to catch up with the changes brought about by its formation. Issues around the formation of DIBP are still working their way through the system.[10] We observed that staff movements have resulted in relationship and knowledge gaps in some of the capability areas. This is evidenced by the significant level of 'acting' staff, the generally short time in which those interviewed had been in their position, or both. As such, corporate knowledge was variable. The development of an endorsed Home Affairs lexicon (as the U.S. DHS has)[11] offers one approach to assistance in overcoming this.

For the purposes of this review, we noted, in particular, that there was an inconsistent understanding of capability within the Department and ABF, across all levels of both organisations. It is important that a shared view of capability is established by all those directly involved with the CLMM. National and international experiences have demonstrated that a holistic perspective, beyond just the procurement of a system or platform, has strong merit. Such an approach would support a more strategic and con-

---

[10] See ANAO, *The Integration of the Department of Immigration and Border Protection and the Australian Customs and Border Protection Service*, 6 June 2018b; Daniel M. Gerstein, Karen Edwards, Julie Newell, and Dulani Woods, *Looking to the Future of the Department of Immigration and Border Protection (DIBP): Assessment of the Consolidation of the Australian Customs and Border Protection Service (ACBPS) and the DIBP (2016–2017)*, Santa Monica, Calif.: RAND Corporation, RR-2262-AUS, 2017.

[11] U.S. Department of Homeland Security, Management Directorate, *Instruction Manual 262-12-001-01, DHS Lexicon Terms and Definitions: 2017 Edition, Revision 2*, Washington, D.C., 16 October 2017.

nected approach to investing in key capability inputs such as people and training, and key enablers such as RD&I, capability development, and critical infrastructure.

Successfully implementing a sustainable CLMM requires an appropriate organisational structure, with capacity built around the competencies of permanent staff. The various elements of the capability lifecycle require different skill sets, both between each of the phases and with those skill sets generally possessed by staff within the Department and ABF. It was noted by officials from the operational, acquisition and policy components of the organisation that, while operators provide a depth of knowledge on how to utilise a capability, once it is delivered to them, those operators were less able to define that capability using a first principles approach.

Similarly, other parts of the organisation require skills in contract management, budget forecasting, cost modelling, operations analysis and systems thinking. While these skills can be brought in from the private sector, those possessing those skills would not have knowledge of the operational environment, the culture of the organisation, and sufficient knowledge on the history of the projects. Examples exist where teams of external providers left at the end of the contract, taking all the corporate knowledge with them as no knowledgeable permanent staff were left (or only one permanent staff person remained). A strategic approach to balancing between in-house and contracted skills is necessary.

The strategy and capability development areas appear to be lacking in both numbers and the array of necessary skills. The entity that currently has responsibility, the Capability Planning and Development Branch,[12] had, as of 17 August 2018, 35 people on the organisational chart, of which there were 19 contractors, 15 permanent staff (including four senior management and administrative roles) and one secondee. Contractors are relied upon are for their specialist knowledge for capability requirements and capability definition activities for the Future Maritime Surveillance Capability project; this could have ramifications once contractors and consultants depart in the event that the Branch is unable to develop sufficient in-house capacity. This has seen some key strategic planning activities effectively outsourced, which could have ramifications once contractors and consultants depart.

We note that the Victoria Police deliberately chose to build a dedicated in-house team of capability development experts when developing and implementing their capability management approach. This workforce stability has ensured improved efficiencies and effectiveness as they cycle through their annual process. As Victoria Police has shown, this does not need to be a large team—their mature model has 25 staff (including operational SMEs) within a 20,000-person organisation and an investment budget

[12] The Capability Planning and Development Branch is responsible for ongoing tasks in relation to the development of submissions to government, assessment of capability, and development of marquee strategies (currently Civil Maritime Strategy) and capabilities (currently the Future Maritime Surveillance Capability).

of approximately $3 billion AUD. Home Affairs may need something slightly larger, given the broader remit of the Portfolio.

A phased rollout for implementation of the agreed approach is necessary to ensure that the Department can build internal competencies in capability development and project management. There are varying levels of maturity in capability development practices and of experience with these practices within the Department. Further, the Portfolio is still in the early phases of its integration with many internal systems (e.g., policy, staffing, culture) and is still developing to meet Department and ABF needs. A phased approach was successfully employed by Victoria Police under similar circumstances, where one functional area applied their new capability management approach over a number of planning cycles. After this proved successful, it was adapted based on lessons identified, and then applied to all functional areas within Victoria Police.[13]

The process of identifying capability requirements and progressing them to the investment approval phase represents a capacity-building opportunity for the Department. Defence employment of immersive methods (e.g., wargames) has proven useful beyond the direct purpose of building the evidence base for decisions, but such methods also broaden participants' knowledge and build relationships across the organisation.

Governance structures tailored to the complexity, size and risk of each program are required to give capability development programs greater agility and assurance. A number of Department and ABF officials suggested that Home Affairs adopt a moderated version of the Defence model for capability development and management. Our analysis suggests that any such model should be carefully tailored to meet the Portfolio's needs, as applying a simplified version of a Defence model may not be viable given some fundamental differences between Home Affairs and Defence. For instance, the available funding instruments are very different (e.g., Defence has a long term endorsed budget of 2 percent of the gross domestic product, with supplementation for operations on a 'no-win, no-lose' model). The two departments have differing operational expectations (e.g., maritime vessel available days for ABF are approximately 300 days per year compared with approximately 120 days per year for Defence). The scale and quantity of projects (e.g., Defence sought approval from government for 111 major projects in FY 2017–2018) is different. The availability of deep capability development expertise is also different, because Defence has a large number of projects which allow staff to build and sustain expertise.

Notwithstanding the limits in flexibility in the use of NPPs as a key funding instrument, we observe that there are opportunities to reflect upon the nature of each new or proposed capability, and determine the level of governance that is appropriate, based on a set of standardised criteria. Defence has recently established the Smart Buyer approach, which uses risk-based thresholds to determine the type of governance

[13] Based on interviewees' comments. See also Victoria Police, 2014.

approach that a project should take.[14] A similar risk-based approach with tailored governance structures is also used by the U.S. DHS for acquisition.[15] A tailored version of the Smart Buyer approach might prove suitable to the Portfolio's needs.

A more collaborative and collegial culture is needed between policy, acquisition and operational staff at all levels, as an essential prerequisite for establishing a resilient CLMM. While it was recognised that the availability of operational SMEs was limited due to the operational tempo, it is acknowledged that the long-term needs of the Portfolio require agency staff to work closely with policy and acquisition staff to establish meaningful capability requirements and ensure that the delivered capability meets the operational needs. This includes all elements of FIC, including training and development. Colocation of operator and policy staff appears to work well, where it occurs.

Decisions about disinvestment have proven challenging, and have not always been made in a timely manner. The immediate impacts on staff can be reduced morale; thus, the need for a unified, corporate position and a clear message to staff on the benefits of disinvestment decisions.

Home Affairs needs to develop and employ a robust and transparent process that incorporates all elements of the capability lifecycle to give the government the confidence it needs for capability investment approvals. The central agencies and Defence have articulated the benefits of building relationships that allow the parties to better understand differing perspectives. A strong strategic narrative could help shape government thinking. Creating time and space for understanding the Portfolio's thinking and contesting the issues could allow the Portfolio to 'test the water' in, for example, an NPP.

Early engagement could extend to inviting the central agencies (e.g., Finance, PM&C) to key investment planning meetings, as is the case in Defence. This would provide the central agencies with visibility of internal funding arrangements, thus providing a more complete view of the Portfolio. This would include funding and staffing pressures. The level and timing of engagement should be informed by the internal resources that the central agencies have at their disposal.

In response to the *First Principles Review*, Defence has stated it 'will focus on planning and governance activities and only do for itself what no one else can do more effectively or efficiently'.[16] Discussions with Home Affairs and ABF officials indicated support for a similar approach within the CLMM. However, to be successful, engagement needs to be described in terms of mutual and national benefit, and on timescales that align with their business cycles. We observe that differences in funding mecha-

---

[14] Australian Government, Department of Defence, 2017.

[15] U.S. Department of Homeland Security, "DHS Instruction 102-01-001, Rev 01 Acquisition Management Instruction," 2016, pp. 26–29.

[16] Australian Government, Department of Defence, undated-a.

nisms and the related issue of funding certainty needs to be treated carefully and discussed openly with government.

Local and international experiences demonstrate that robust RD&I programs are essential for future-proofing Home Affairs as such programs enable the exploration, acquisition and integration of new capabilities within dynamic environments. The 2016 DIBP *Technology Review* noted

> the current technology environment is characterised by bespoke, point solutions designed to meet the needs of a specific business area, rather than the broader department. Bespoke systems are more expensive to maintain and result in unnecessary duplication of capabilities. They are also much harder to upgrade to the evolving business needs, operational requirements, or legislative changes. The Departments' technology is also experiencing increasing levels of 'technical debt' which is the additional workload and cost required to sustain aging technology which is not upgraded or replaced.[17]

Many interviewees confirmed this and provided examples of staff choosing replacement technologies based on very narrow market surveys, rather than conducting a more comprehensive assessment of available options. Suggestions were made about leveraging the capabilities of other departments or seeking market input, though this appeared to be on an as-needed basis, apart from a couple of instances. [18]

While it was recognised that the Department did not currently have the resources to establish its own fully-fledged RD&I capability (such as those that exist in Defence or DHS), it was less clear on how this was being addressed within the CLMM. DIBP developed a strategy for technology;[19] however, that strategy was largely focused on ICT.

We note that there is work underway to address this challenge. The recently released report, *National Security Science and Technology Policy and Priorities*, identifies six high-level priorities that are relevant to the Portfolio,[20] although there is no detail on implementation other than an interdepartmental committee. We are aware that the Department is developing a framework for a Science and Technology Strategy. We emphasise the importance of linking this to strategic objectives, functions and tasks, so that this strategy can be properly considered and investments prioritised as part of the broader investment plan. We also note that a previous document, the *National Security*

---

[17] Australian Government, Department of Immigration and Border Protection, 2016.

[18] It is noteworthy that Defence has now established and funded an Innovation Hub to complement its existing Research and Development group.

[19] Australian Government, Department of Immigration and Border Protection, *Technology Strategy 2020*, 2017d.

[20] Australian Government, *National Security Science and Technology Policy and Priorities*, Defence Science and Technology, 2018.

Science and Innovation Strategy,[21] developed within PM&C via an interdepartmental process that included the AFP and ASIO, is structured along these lines. This strategy identified strategic priorities (e.g., 'a more prepared and resilient society'), linked these priorities to a set of 12 objectives (e.g., 'to enhance the ability of our physical infrastructure to withstand attack or damage and remain functional'), and established a number of tasks for achieving each objective.[22]

All peer organisations are also addressing this issue, with UKHO and Home Affairs on a similar trajectory in developing and implementing a capability framework. The United Kingdom is slightly more advanced. In reviewing capability development among peer organisations, it became clear that the opportunities, challenges and concerns faced by Home Affairs mirror those of other organisations. Therefore, while circumstances may differ across these groups, we observe that all are seeking to establish a robust, transparent and forward-looking approach to building their capabilities. From interviews with UKHO officials, particularly their depictions of the emerging Home Office Strategic Planning System,[23] it is clear there are close parallels between the UKHO and Home Affairs in terms of the demands on their systems. This is not surprising, given that the Home Affairs Portfolio design was based upon the UK model.[24]

From the CLMM perspective, both portfolios consist of a highly complex landscape of semi-independent agencies, departments, and actors with their own budgets and overlapping governance responsibilities; both have variable approaches to, and quality of, planning across their portfolios; both have pressures to operate with greater efficiency and effectiveness; and both face questions about how to leverage and build capability across the department. The UKHO is in the early stages of developing a strategic planning framework, and lessons from its experience in the coming months and years could be valuable, particularly when planning for implementation.

Historically, the UKHO approach to strategic planning has been short-term (covering the following three years) and bottom-up, rather than taking a systems approach, working with wider partners, and identifying threat-agnostic capabilities. There is also no common UK procurement agency (outside of MoD), suggesting that procurement in the areas of responsibility of the UKHO can be piecemeal. We also note that the term 'capability' and the concept of capability development are not widely used in the UKHO, although these concepts are used in MoD. As part of the emerging Home Office Strategic Planning System, the concepts of capability development thinking are now being used by senior officials in the UKHO.

---

[21] Australian Government, *National Security Science and Innovation Strategy*, Department of Prime Minister and Cabinet, 2009.

[22] Australian Government, 2009, pp. 10–14.

[23] UKHO is currently developing a new strategic planning framework.

[24] For instance, see the introductory remarks from Secretary Pezzullo in Parliament of Australia, 2018.

The UKHO portfolio approach to capability management is under development. The UKHO is 18 months into the development of its new 'organisationally agnostic' Strategic Planning Operating Model. The UKHO has recognised that a significant challenge in adopting this model will be organisational culture and incentives to change. Human factors and incentives are considered to be more important than the content of a common framework for capability. The UKHO views the key as shaping an environment in which actors are motivated to participate in joint capability identification and definition.

APPENDIX G

Strategic Planning Phase

This appendix describes the taxonomy and frameworks for the strategic planning phase of the CLMM. Noting the developing maturity of the Home Affairs CLMM, simple and mature models are provided. Before describing the detailed framework for the strategic planning phases, it is important to describe the overall classification that will be employed within this appendix.

G.1 Definition

As noted in Chapter Two, the Department's current definition of strategic planning is:

> Strategic planning, the first stage, focuses on strategy and its role in informing and shaping capability development. It provides a view of the Department's present and future direction to inform forward planning of operational and capital investment.

Analysis of the terms of reference, discussions with senior staff, and reviews of relevant documentation suggest that the definition of strategic planning provided by the Department (see Chapter Four) does not capture the requirement for strategic planning within the Home Affairs context. We have developed the following working definition, based on our initial observations of international best practice:

> Strategic planning, the first stage, focuses on strategy and its role in informing and shaping capability development. It provides a risk-based view of the Department's present and future direction to inform forward planning of investment across the life of a capability, including acquisition, operations, sustainment and disposal.

For the purposes of this study, the strategic planning stage aims to develop a strategy-led auditable process that links government guidance, through strategic objectives and operational tasks, to capability needs. This is achieved through a capability framework that seeks to minimise strategic risk while exploiting emerging opportunities. In a mature model, such as that employed by Defence, it links government guidance, the current and future strategic environment, and portfolio structural arrange-

ments to identify the capability partitions needed to best achieve the principal tasks that underpin achievement of the strategic objectives.[1] The output of this phase is capability sets which are defined in terms of capability needs (assessed against principal tasks), the risks associated with these capability sets, and the emerging operational environment.

Figure 4.4 outlines a simple taxonomy that underpins the strategic planning phase. Simply put, the objectives describe why something should be done, the tasks describe how it should be done, the functions describe what should be done, and the capabilities (supported by key enablers) define with what it should be done. Given the varying levels of experience in capability lifecycle management within Home Affairs, Figure 4.4 is a worthwhile reference tool to ensure that there is a common understanding of key terms across all elements of the Department and Portfolio. The remaining sections in this appendix define the framework in which the objectives, tasks, functions and capabilities are employed.

G.2 Logic Model

One of the first requirements of a holistic investment program is to ensure that the investment strategy implements government policy, and that there is clear traceability between the two. The first step in developing an auditable and transparent process between government guidance and capability requirements is to develop an auditable process to derive operational tasks from government guidance. For this analysis, we utilise a strategy-to-task framework. This step will ensure a broad alignment with the way in which Defence develops and represents its capability development framework to government and the central agencies.[2]

Strategy-to-task frameworks have been applied to similar areas in Home Affairs, to ensure that operational capabilities have strategic underpinnings. This framework is centred on the need for traceability from capability requirements (phase 2 in the CLMM) and 'the tasks, conditions, standards, missions, threats, and overall strategic guidance'.[3] This approach has been employed in public sector entities since the 1990s, as it allows a direct mapping between government guidance and the operational tasks that need to be accomplished to deliver on that government guidance.[4] Once the operational tasks have been established, the capabilities to meet those tasks can be determined.

---

1 De Spiegeleire, 2011, p. 22.

2 Examples of central agencies include the Department of Finance and the Department of Prime Minister and Cabinet.

3 "Program Management," in Defense Acquisition University, undated.

4 See Thaler, 1993.

The upper half of Figure 4.2 provides a mature strategy-to-task logic model that can be applied to the Portfolio. It would form the basis of the strategic planning component when Home Affairs is undertaking the major capability development review. This logic model depicts the Australian Constitution and legislation as key framing elements of government guidance, as government guidance will need to be consistent with the Constitution and legislation. It should also be noted that both the Constitution and legislation are predominantly enduring and constant, regardless of the geopolitical environment. From government guidance, strategic objectives, operational objectives, and operational tasks can be derived. Within this framework, objectives are the effects that the Portfolio is trying to achieve, with the likelihood that several elements of the Portfolio will contribute to achieve the same objective. Specifically,

- strategic objectives define the emphasis across the Portfolio and outline the Portfolio objectives
- operational objectives define the weight of effort over time among operational objectives, and define the weight of effort among operational tasks
- operational tasks define how to accomplish the operational objectives
- organisational functions describe the key roles that the Australian government has asked Home Affairs to perform.

Further, government guidance will also determine the resources available to the Portfolio and the context in which investment decisions should be made. While the resource implications of capability decisions should be considered while capability options are being developed, the context within which the Portfolio operates (i.e., current security risks, emerging threats, potential future operational landscapes) should form a key component of strategic objectives, operational objectives and operational tasks.

The upper half of Figure 4.3 provides a simplified strategy-to-task framework that could be used by the Department as an interim model as its capability development processes, systems and capabilities mature. Once they are mature, the framework could be used for the annual strategy update, where Home Affairs determines whether and how changes (e.g., to the strategic context or government guidance) are significant enough to necessitate adjustments to capability needs. The assumption here is that those changes are not significant; however, that would be a decision for the SES, as the most likely cause for a major review is significant changes to the strategic environment.

G.3 Testing the Model

To determine whether the model is fit for purpose, we have developed a worked example of the frameworks depicted in Figures 4.2 and 4.3, based on publicly available

Table G.1
Strategic Objectives Example

Strategic Objectives		
Prosperous: Through our unique capabilities, powers, and activities, we contribute to Australia's prosperity by enabling a globally connected and open economy and society.	Secure: Together, we will protect Australia and Australians from key national security and criminal threats.	United: We celebrate Australia's multicultural society and safeguard our democracy by building community resilience and engendering respect for Australia's shared values and institutions, our way of life, and the rule of law

SOURCE: Based on Australian Government, Department of Home Affairs, 2018a, p. 11.

information. It should be noted that a more-holistic population of these frameworks should be subsequently determined in consultation with key stakeholders. It should also be noted that the examples used in this appendix include some roles and responsibilities that pertain to portfolio agencies, in order to consider the broader implications of the proposed framework.

The *Blueprint for Home Affairs* states three strategic objectives for the Home Affairs Portfolio.[5] These objectives are provided in Table G.1.

There are a number of operational objectives and operational tasks that the Portfolio must achieve in order to achieve the strategic objectives described in Table G.1. Examples of these operational objectives and tasks, based on publicly available information,[6] are defined in the following figures, both for the mature (Figures G.1–G.3) and interim (Figures G.4–G.6) strategic planning logic models.

Organisational Functions

Organisational functions describe the key roles that the Australian government has asked Home Affairs to perform. By way of example from the open literature, Table

[5] Based on Australian Government, Department of Home Affairs, 2018a, p. 11.

[6] See Australian Government, Department of Home Affairs, *Portfolio Budget Statement 2018–19 Budget Related Paper No. 1.10 – Home Affairs*, 2018d; Australian Government, Department of Home Affairs, 2018a; and Dutton, 2018.

Figure G.1
Mature Prosperous Strategy to Task Mapping Example

Strategic objective 1	Operational objectives	Operational tasks
Prosperous: Through our unique capabilities, powers and activities we contribute to Australia's prosperity by enabling a globally connected and open economy and society	Facilitate legitimate trade	Deter, disrupt, detect and investigate the unauthorised trade across the border continuum
		Facilitate legitimate trade and the movement of goods to contribute to a strong economy
		Effective collection of revenue, detection of revenue evasion and compliance with laws
		Identify and manage trade risks across the border continuum
	Facilitate legitimate travelers and migrants	Assist skilled migrants contribute to a strong economy
		Deter, disrupt, detect and investigate the unauthorized movement of people across the border continuum
		Facilitate the travel and stay of people to contribute to a strong economy
		Identify and manage migration risks across the border continuum

Figure G.2
Mature Secure Strategy to Task Mapping Example

Strategic objective 2	Operational objectives	Operational tasks
Secure: Together, we will protect Australia and Australians from key national security and criminal threats	Counter terrorism	Counter offshore terrorism activities
		Control the return of foreign fighters
		Counter domestic terrorism activities
	Counter serious and organised crime	Counter transnational serious and organised crime
		Counter domestic serious and organised crime
		Counter offshore serious and organised crime targeting Australians
	Counter espionage, foreign interference and malicious insiders	Protect Australian secrets
		Protect Australian sovereignty
		Protect Australians who may be vulnerable to coercion from hostile state actors
		Ensure integrity of Australian government business

Figure G.3
Mature United Strategy to Task Mapping Example

Strategic objective 3	Operational objectives	Operational tasks
United : We celebrate Australia's multicultural society and safeguard our democracy by building community resilience and engendering respect for Australia's shared values and institutions, our way of life, and the rule of law	Strengthen social cohesion	Build strength in diversity and social participation
		Targeted work with vulnerable communities and institutions
		Diversion and deradicalisation
	Manage effective migration and citizenship programs	Manage the intake of places for migration and citizenship to contribute to a cohesive society
		Contribute to the global management of refugees and displaced persons deradicalisation
	Build disaster resilience	Build resilience for large strengthening emergency response
		Build resilience for aviation, maritime and national security threats
		Build resilience for public spaces

Figure G.4
Interim Prosperous Strategy to Task Mapping Example

Strategic objective 1	Operational tasks
Prosperous: Through our unique capabilities, powers, and activities we contribute to Australia's prosperity by enabling a globally connected and open economy and society	Deter, disrupt, detect, and investigate the unauthorised trade and movement of people across the border continuum
	Facilitate legitimate trade and the movement of goods, and people to contribute to a strong economy
	Effective collection of revenue, detection of revenue evasion, and compliance with laws
	Identify and manage trade risks and migration risks across the border continuum
	Assist skilled migrants contribute to a strong economy

Figure G.5
Interim Secure Strategy to Task Mapping Example

Strategic objective 2	Operational tasks
Secure: Together, we will protect Australia and Australians from key national security and criminal threats	Control the return of foreign fighters
	Counter transnational serious and organised crime
	Counter offshore terrorism and serious and organised crime
	Protect Australian secrets and sovereignty
	Protect Australians who may be vulnerable to coercion from hostile state actors
	Ensure integrity of Australian government business
	Counter domestic terrorism and serious and organised crime

Figure G.6
Interim United Strategy to Task Mapping Example

Strategic objective 3	Operational tasks
United: We celebrate Australia's multicultural society and safeguard our democracy by building community resilience and engendering respect for Australia's shared values and institutions, our way of life, and the rule of law	Build strength in diversity and social participation, including diversion and deradicalisation
	Targeted work with vulnerable communities and institutions
	Manage the intake of places for migration and citizenship to contribute to a cohesive society
	Build resilience for large-scale natural hazards, including strengthening emergency response
	Build resilience for aviation, maritime and national security threats
	Contribute to the global management of refugees and displaced persons

G.2 provides an overview of the functions performed within the Home Affairs and a description of them. Each of the operational tasks may include some, or all, of the functions listed below.

Capabilities

Although there are many different definitions of capability, we have used the definition for capability within this report as described in Chapter Three. Under this definition, a capability is defined in terms of the effect or outcome it produces, rather than in terms of a piece of equipment. Ensuring that capabilities are defined in terms of the effects they produce will ensure that the full possible range of acquisition solutions can be considered, rather than narrowing down these options too early in the CLMM. Table G.3 provides an example of the type of capabilities that could apply to the Home Affairs Portfolio.

Table G.2.
Examples of Home Affairs Functions

Function	Description
Border Protection	Protect Australia's border through the detection and deterrence of and response to the illegal movement of people, illegal fishing and natural resource exploitation, and the illicit movement of prohibited goods and commodities.
Immigration, Citizenship and Multicultural Affairs	Provide citizenship and temporary and permanent migration programs, and manage the refugee and humanitarian programs.
Customs	Control the movement of people and goods across the border, while facilitating legitimate trade and travel.
Critical Infrastructure Security	Protection of those physical facilities, supply chains, information technologies, and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security.
Transport Security	Make sure Australians and our national interests are secure through regulation that supports industry and the community as they carry out trade and travel activities.
Emergency Management	Lead Australian disaster and emergency management activities through the delivery of critical programs, policies and services that strengthen and maintain Australia's national security and emergency management capability.
National Security	Protect Australians and their interests by working with national and international security partners to prevent harm from occurring.
Commonwealth Law Enforcement	Lead law enforcement efforts to keep Australians and Australian interests' safe both at home and overseas.
Coordination	Lead national efforts by coordinating cross-agency policy and program development.

SOURCE: Based on Australian Government, Department of Home Affairs, 2018a.

Table G.3
Example of Home Affairs Capabilities

Category	Capability
Intelligence	Intelligence collection
	Intelligence analysis
	Intelligence fusion
	Intelligence assessment
	Intelligence dissemination
Cybersecurity	Cyber prevention
	Cyber detection
	Cyber deterrence
	Cyber response
Physical security	Community policing
	Protection of people or assets
	Prevention
	Deterrence
	Investigation
	Prosecution
Surveillance and response	Aerial surveillance
	Maritime-based surveillance
	Onshore surveillance
	Maritime-based response
	Onshore response
Border clearance	Cargo clearance
	Passenger clearance
	Aircraft clearance
	Vessel clearance
Immigration detention and regional processing	Onshore detention and processing
	Regional processing and placement
	Transfers and removals
Immigration and international visitor administration	Migration program management
	Visa and citizenship processing
	Refugee and humanitarian assistance
	Multicultural program delivery

APPENDIX H

Capability Requirements Phase

This appendix describes the definitions and frameworks for the capability requirements phase of the CLMM. It provides a definition that captures the intent of this phase, details the framework that commences with the outputs of the strategic requirements phase, and transitions this to the product of capability requirements phase, namely, a 10-year capability plan. It will also provide a mechanism for the entry of new requirements, based upon their complexity, scale or underlying risk.

H.1 Definition

As noted in Chapter Two, the current definition of capability requirements is the

> capability requirements [phase] is the point at which high-level capability gaps are identified, and proposals are reviewed and prioritised for funding, either externally via a New Policy Proposal or internally through the Departmental Capital Budget.

We note that the intent to consider the entire program and the range of funding instruments that operate within the Portfolio makes the provided definition redundant, since it focuses explicitly on only two of the 11 existing funding instruments currently present within the Portfolio. We observe that Defence has previously defined this as the Needs phase, and specified that 'Government endorses the need to address the identified gaps by approving the inclusion of a capability project, with an indicative budget provision'.[1] Based on these considerations, we developed the following working definition for the capability requirements phase:

> Capability requirements is the point at which high-level capability gaps are identified, prioritised and endorsed. Capability proposals (incorporating capability needs statements and indicative budget provisions) are developed, and likely funding mechanisms identified, either externally via funding instruments such as a New Policy Proposal, or internally through the Departmental Capital Budget.

[1] See Australian Government, Department of Defence, 2012a, p. 4.

For the purposes of this study, the capability requirements stage of the CLMM will result in an identification and risk-based prioritisation of capability gaps; an understanding of the operational means of addressing or managing those risks and gaps; the establishment of a 10-year capability plan (including current and planned capabilities) with, at a minimum, estimated through-life costs for each capability, critical decision points, identification of potential overlaps, and interdependencies; and a strategy of engaging other departments and government (as necessary).

H.2 Framework

With the capability needs identified as a broad response to a capability gap, it is now possible to progress towards developing a long-term plan for developing the capability requirements that address these capability gaps. A mature framework for determining the capability requirements from the operational tasks and the Portfolio functions is shown in the lower half of Figure 4.2.[2] As noted earlier, this activity is resource-intensive, and we would recommend it be completed when the Department is undertaking a major capability development review, although there is nothing precluding Home Affairs from enacting this approach, even if the interim strategy-to-task approach is taken in the strategic planning phase of capability identification.

Given that the mature model (lower half of Figure 4.2) will require a significant investment of resources, we also propose a simplified version of this as an interim measure (Figure 4.3). This model aligns with CBP approaches that focus on a singular operational task, which linked *needs* for that task to *options*, tested through *mission* (context from our perspective) and *choices* (i.e., the capability plan).[3] The simplified approach can act as an interim approach to meet the needs of Home Affairs as it develops staff capacity, corporate knowledge, information systems, and analytical tools needed to build and maintain a long-term capability plan. It would also be suitable for use in the years between the major capability development reviews, since each step would focus on adjusting the current elements (i.e., existing gaps and opportunities, options, resource estimates) in light of changes identified in the strategic planning phase.

Establishing Capability Roadmaps for Functional Areas

The capability requirements phase commences with the identification of capability gaps and opportunities. These are established by mapping the existing and planned capabilities to the capability needs (identified during the strategic planning phase).

---

[2] The is based upon the standard CBP approaches (e.g., Technical Cooperation Program, 2004) and their application in a Defence context (e.g., Australian Government, Department of Defence, 2012a).

[3] See for instance, Davis, 2002.

In each case, evidence is collected and analysis to allow judgements to be made as to whether, over the next ten years, Home Affairs will have sufficient capabilities to deliver the outcomes and effects to meet capability needs. This analysis should also distinguish whether the need is partially met, and, if so, the basis for the shortfall. There may also be examples where multiple capabilities meet the same need or are required to work together to meet a need. These examples must be captured, as they provide a basis for identifying disinvestment opportunities and interoperability risks. The choice on how to describe emerging gaps and opportunities is important. They should be described consistently, and in a way neither suggests a potential solution nor precludes other feasible options.

The full set of gaps and opportunities are then prioritised using a structured analytical approach. At its simplest, this might take the form of an expert opinion-based multicriteria decision-analysis approach,[4] when comparative assessments are made against a standardised set of risk-based criteria that are derived from strategic and operational drivers. Such an approach ensures consistency, both within a cycle and across annual cycles, potentially reducing the overhead in performing this analysis; highlights any biases that might emerge during the assessments; and provides a transparent evidence trail that underpins the future acquisitions. As its capability and knowledge base strengthens, Home Affairs should make a conscious choice to employ more-robust analytical approaches (such as analytical hierarchy processes, desktop wargaming, Delphi analysis, and simulation)[5] to strengthen the evidence base, particularly when performing the major reviews.

Concurrent with this activity is the development of functional strategies and concepts of operations across the functions identified in the strategic planning phase.[6] Narrative in nature, these strategies and concepts are developed by describing each function in terms of what its long-term requirements are, given the feasible future environments. At a minimum, those futures should incorporate forecasts of political, economic, social and technological changes across a one- to two-decade horizon. There are a number of standard analytical techniques that can support this.[7]

---

4 Currently used by both Defence and Home Affairs.

5 See, for instance Paul Goodwin and George Wright, *Decision Analysis for Management Judgement*, John Wiley and Sons: Chichester, UK, 1998; and N. K. Jaiswal, *Military Operations Research: Quantitative Decision Making*, Springer: New York, 1997.

6 For instance, see examples of these for Transport Security, e.g., Australian Government, Department of Infrastructure and Regional Development, *Transport Security Outlook to 2025*, 2017b.

7 See for instance, Marjolein B. A. van Asselt, Susan A. van 't Klooster, Phillip W. F. van Notten, and Livia A. Smits, *Foresight in Action: Developing Policy-Oriented Scenarios*, Routledge: London, 2010.

Mapping the prioritised gaps and opportunities to functions, and in turn, to the relevant strategies and concepts, [8] will identify prioritised capability goals that Home Affairs needs to address, and the timeline for when they need to be addressed. Understanding the timeline of the capability lifecycle is important, as it provides Home Affairs with forewarning of future gaps created; for instance, when an existing capability reaches the end of its life. This step provides senior executives with the evidence base to be proactive in deciding when and where to invest, where there is likely to be insufficient investment, where there might be opportunities to disinvest from existing or planned capabilities, and where adjustments to 'in-flight projects' can be made.[9] Senior management would consider this and prioritise which of these capability goals requires further consideration, and the level of detail for each. This represents an approved set of function-based capability roadmaps for Home Affairs.

Capability Options

Decisions are then made as to which of the capability priorities are to be explored in greater depth. Best practices recommend the development of broad capability options for addressing the high-priority gaps and opportunities outlined in the capability roadmap.[10] For instance, a maritime surveillance capability could take the form of a piloted or unpiloted vehicle. In addition, it could be seaborne, airborne or operated from space. It might employ different suites of tools to perform its surveillance, data fusion, transmission and analysis functions. Further, creating diverse options allows for the exploration of distinctively different alternatives to addressing a gap or realising an opportunity. Further, the options should not focus purely on materiel solutions (e.g., systems and platforms). Rather, consideration should be given to trying to fill the capability gaps or opportunities through such nonmateriel means as other FIC elements: organisation, people and training, or a combination of materiel and nonmateriel means.[11] This, again, emphasises that a capability is created through a range of inputs (i.e., FIC) and solutions should be constructed in those terms, rather than treated as a platform or system.

These options are tested against an endorsed set of planning scenarios to evaluate their relative utility when embedded within the broader enterprise capabilities: both

---

[8] Some gaps and opportunities might affect multiple functions. These impacts should be captured, as they may become relevant during the balance of investment activity.

[9] 'In-flight projects' is the terms used within the Department to reference those projects that have DCB or NPP funding.

[10] "Analysis of Alternatives, Cost Estimating and Reporting," in Defense Acquisition University, undated. Here we distinguish capability and acquisition options. For the latter, the capability is well defined (the capability option has been chosen) and the choice is between different potential providers of elements of that capability—for instance of a ship. These investment options are the focus of the capability definition and investment approval phases.

[11] "Program Management" in Defense Acquisition University, undated.

those that currently exist and those that are planned. For some areas within the organisation, this may be relatively straightforward as they operate largely independent of other areas. However, other areas will prove to be more challenging. A scenario-testing activity will minimise the risk of perverse outcomes, and is one example of why the simple model is not sustainable in the long run.

To ensure the feasibility of each capability option, best practice recommends that a comparative analysis of each option should be performed.[12] Such a comparison enables decisionmakers to select a preferred capability solution by assessing its relative effectiveness in meeting the capability need against resource demands associated with each option. Such an analysis should include information on (and potential undertake separate analysis of) the following:[13]

- the capability gaps and opportunities being addressed, including the time frame
- the threat and operating environment
- underlying assumptions, constraints and limitations
- the effectiveness of each alternative in filling the capability gaps
- cost estimates of the total lifecycle cost of each alternative, including costs for development, production, operations and support, and disposal
- risk analysis, including any risks not already addressed.

Forecasting resource demands may not be straightforward, as it incorporates both budget and personal requirements well into the future for options that are not fully formed. These can be established using analytical approaches such as parametric modelling or trend analysis. We note that Defence previously used estimates of NPOC[14] within capability proposals.[15] A timeline that includes such key decision points as the retirement date for an existing capability and when government decision is required is also necessary. We note that a tailored approach can be taken here, so that projects of lower complexity, risk or scale can utilise a simpler approach (such as a market survey).

Balance of Investment Review

Given that Home Affairs represents a complex, interdependent system of cooperative (and sometimes competing) capabilities, it is necessary to regularly consider the system in its entirety. This is the BoI review (see Figure 4.2), which tests the anticipated future

---

[12] See, for instance, "Analysis of Alternatives, Cost Estimating and Reporting," in Defense Acquisition University, undated; Davis, 2002, p.3.

[13] "Analysis of Alternatives, Cost Estimating and Reporting," in Defense Acquisition University, undated.

[14] NPOC estimates are determined by calculating the difference between the current personnel and operating costs associated with an existing capability, and those estimated for the capability options. Given personnel and operating costs often represent the main difference in cost drivers, it provides a consist and straightforward mechanisms to estimate resources for less complex projects.

[15] See Australian Government, Department of Defence, 2012a, pp. 15–16.

enterprise (current, planned and proposed capabilities) given various funding assumptions. In CBP language, BoI is defined as[16]

> evaluating the requirements of the defence force in terms of cost, capability and schedule within applicable constraints. It requires the synthesis of the key findings developed across all capability partitions. Out of the BoI exercise, a framework for investment should be developed. This serves as the basis upon which defence develops its strategic investment or capability development plan.

BoI analysis can take a number of forms. The most comprehensive form would be to look across the entirety of the enterprise, including all capabilities. This can be difficult, particularly for the first iteration, as the demarcation between functional areas can be problematic. A better approach would be to allocate resources to each functional area and allow them to perform their own balance of investment analysis and employ analytical tools and techniques appropriate to their functional area.[17] In this case, the final integration is a two-step process. The first element is focused only on those areas where there is significant overlap. Once that is complete, committee-centred approaches, supported by appropriate decision-support tools, are employed to explore the strategic and enterprise risks to Home Affairs across, at minimum, the next decade. This might include selecting capability options that were not originally supported in the previous step. The step concludes with recommendations on what should be included, given different funding choices.

Ideally, all capabilities would be considered independently of functions. However, the reality is that while this will limit interoperability across functions, the knowledge, experience and data gained through early iterations will better position Home Affairs to take a more comprehensive approach. We observe Victoria Police took such an approach by initially focusing on one functional area, iterating through this a couple of times, and then extending to the entire enterprise.

Capability Plan

Once the options for each capability are agreed upon, these can be integrated into a long-term capability plan. We recommend a 10-year plan, as this looks far enough beyond the forward estimates to ensure a comprehensive understanding of the longer-term capability and financial issue, but not too far as to go beyond the lifecycle associated with the planning, acquisition and retirement of most capabilities relevant to Home Affairs. We note that a 10-year horizon also aligns with the time horizon that Defence employs,[18] ensuring that the government is able to consider Australia's long-

[16] See Technical Cooperation Program, 2004, p. 13.

[17] See Technical Cooperation Program, 2004, p. 13.

[18] For instance, see Australian Government, Department of Defence, 2012b; Australian Government, Department of Defence, *2016 Integrated Investment Program*, 2016c.

term security capability requirements (Defence and National Security) in a consistent matter.

Each capability option proposal that is selected for inclusion in the capability plan would have a designated project title, functional area, owner (at the SES-2 level or equivalent), and a brief description of the scope of the option. It would also have an appropriate time frame for initiation, key decisions, acquisition, operational use, and disposal. For projects for which development has already commenced and those already operational, the resource implications (by FIC), broken out on an annual basis, are required. For new projects, simple modelling that estimates resource implications is necessary. In all cases, the resources should be broken down by phase (i.e., development, acquisition, sustainment, disposal) and the expected funding source for these phases (e.g., NPP, DCB). The project description should include possible overlaps, interoperability issues, and opportunities to realise synergies between projects.

It is important to note that the final capability plan is not simply a collation of the project list. Therefore, before finalising the capability plan, it is important to determine whether the anticipated long-term resource requirements are affordable in the short term, or create unacceptable risks in the medium to long term. Further analysis should be done to determine if there are specific risks associated with schedules, interdependencies and capability gaps. This may require some iterations through the capability plan in cases of unacceptable risk. Once this process is completed, recommendations for the initiation of new projects for inclusion in the integrated investment program would be made, along with the resources necessary to support the development of the business cases through the (following) capability definition phase. This would require approval from senior committees within Home Affairs and then would be incorporated into the Budget and Corporate Plans.

From an implementation perspective, we note that considerable effort is required to institute this framework across all organisational functions. As such, we recommend that Home Affairs identifies all the capabilities that would be included on the capability plan. This could be based upon the output from the Capability Baseline Review, the current five-year investment plan, approved business cases, and existing capability roadmaps. We would then recommend a staggered approach, whereby the complete details are included in a limited number of areas (e.g., where there is high project complexity, cost or risk) and new projects. For the remaining project, we would recommend extending a 'funding wedge' beyond their five-year limit. Finally, we note that once Home Affairs develops a comprehensive capability plan, there should be an annual review to update the information and make changes on a 'by exception' basis. We would recommend that a fundamental review of the capability plan only occur when the there is a significant update to the strategic plan.

H.3 Governance

To meet government expectations for the effective management of risk within the public sector, Home Affairs will need to incorporate a risk-based approach, regardless of which governance framework is chosen. As the ANAO has noted, 'the effective management of risks assists Commonwealth entities and companies to set and achieve strategic objectives; comply with legal and policy obligations; improve decision-making; and allocate and utilise resources'.[19] In addition, as a result of the *First Principles Review*,[20] Defence instituted a Smart Buyer framework to determine the level of oversight required for each capability development project. Smart Buyer is a principles-based process to ensure that the right questions are asked at the early stages of a program or project. Within this framework, a risk-based approach is employed, where assessments of 12 key risks are conducted and inform the level of oversight required within Defence.

The Smart Buyer framework represents an approach that can be used to standardise the criteria by which all capabilities and their options are defined and their maturity assessed. Table 4.1 represents assurance criteria, so that senior management can be confident that a capability option is mature enough to be considered for the capability plan. The assurance criteria are based upon the descriptions used by Smart Buyer, and can be characterised within a risk-based approach whereby both the enterprise risks—top-down (strategic alignment), bottom-up (operational alignment) and middle-out (external constraints)—and project risks—effects (benefits realisation), technical (technological maturity), cost (financial viability) and schedule—are captured.[21] We note that the current Home Affairs business case template explicitly seeks to capture both risk areas.

We recommend a capability development risk register be established to capture and monitor these risks from this CLMM phase to capability disposal. By incorporating the risk register with the criteria above, Home Affairs is meeting best practices in risk management,[22] in a manner consistent with central agencies and the government's requirements. Further, it can provide a basis for common understanding in cases where support might be sought from Defence.

---

[19] ANAO, "The Management of Risk by Public Sector Entities," 15 August 2017.

[20] Australian Government, Department of Defence, 2015.

[21] For instance, Australian Government, Department of Finance, 2016a.

[22] See Australian Government, Department of Finance, 2013.

H.4 Summary

Taken together, strategic planning and capability requirements ensure that the 'right' problems, issues and challenges are being addressed. Without this, capability solutions risk being ineffective, inefficient, and not focused on the highest priority risks. In this appendix, we described the approach for linking the capability needs (as established based on government guidance) to a long-term capability plan. Such an approach will enable Home Affairs to better prioritise its needs and inform government about these needs. Importantly, it provides the ability to foreshadow the opportunity cost of investment choices to government and the central agencies.

APPENDIX I

Capability Definition Phase

This appendix describes the definitions and frameworks for the capability definition phase, the first part of capability design. It defines what is required during this phase, and then details how to transition from the capability plan to the integrated investment plan.

I.1 Definition

As noted in Chapter Two, the current Department definition of capability definition is as follows:

> Capability definition encompasses the development of business cases to support prioritisation of proposals only seeking external funding.

We believe this definition is too restrictive, as it does not allow for a comprehensive picture of the Department's and ABF's (and potentially the Portfolio's) investment plan. A number of senior officials from within the Department and ABF provided examples of how a focus on NPPs led to an underinvestment in the through-life and disposal costs of existing capabilities.[1] This definition also does not allow a true balance of investment, since options for addressing capability gaps might utilise some of the existing 11 funding instruments across the Portfolio. Further, it does not allow for the development of a strong relationship with other departments and government, as they will not be able to gain a comprehensive understanding of the Home Affairs strategy. Based on our review to date, we have developed the following working definition, which will be adjusted as the project progresses:

> Capability definition encompasses the establishment of capability proposals, the development and exploration of options for addressing the capability requirements,

[1] Quantitative evidence for this falls into the remit of another activity within the Capability Review.

and the development of business cases to support prioritisation across a multiyear integrated investment program.

In essence, the capability definition phase of the CLMM acts as the bridge between the aspirational long-term capability plan and the forward-estimates investment plan for capability.[2] Capability definition establishes a program management environment which decouples the capability requirements into discrete projects. Here we differ from the current starting point for projects within Home Affairs. The current approach is that a project only exists within the capability delivery phase, and starts once funding has been allocated.[3] This is not consistent with the practices of other similar organisations and creates unnecessary constraints on managing the capability lifecycle. Initiating the project at this point shows recognition that there are resource implications in developing the business case for a capability, allows a consistency in approach, demonstrates opportunities to better understand interdependencies, and removes the risk of stovepipes between projects. Further, the recommended approach provides continuity across the entirety of the capability lifecycle.

For each project, details developed through the development of the initial business case and other supporting documentation allow a prioritisation process to inform acquisition decisions and through-life support through a multiyear integrated investment plan (currently limited to five years in the Department). The output is a set of prioritised capability projects described in terms of the desired capability posture, each with an investment approval strategy based on its inherent complexity, an agreed multiyear funding envelope (including estimation of any operation, sustainment, and disposal costs beyond the investment plan), and any interdependencies between projects. Amendments to the existing acquisition, sustainment and disposal plan (including disinvestment) would also result from this phase. Finally, investment plan identifies and, once endorsed, releases the internal resources necessary to develop the final business cases and conduct the acquisition.

I.2 Framework

Unlike the strategic planning and capability requirements phases, we suggest a single logic model for the capability definition phase (Figure 4.5). This would demonstrate that Home Affairs follows international standards for program and project management. The role of CM, who is responsible for overseeing and coordinating across all

---

2 In effect, this integrated investment program represents the application of the first five years of the capability plan.

3 Australian Government, Department of Home Affairs, "Project Management Framework 'At a Glance,'" version 4.40, internal document, 2018e.

projects that that are assigned to them, is critical.[4] CMs represent each of their projects during program prioritisation, and contribute to the collective decision to endorse the integrated investment program. It will be the responsibility of the CM to calculate the effort required for each step based on the underlying complexity and risk associated with each project. In developing the logic model for the capability definition phase, we observe that the Department established a five-year integrated investment plan for FY 2018–2019. While this was not based on a capability plan (the Department identified capability gaps and then prioritised these gaps to establish an investment plan), it does demonstrate that the Department has some of the key processes in place.

Project Initiation

The first step in the capability definition phase is project initiation. Building on the information collected in the capability requirements phase, this requires the assigned CM to reconfirm the underlying capability need that the project is to fulfil, identify the project manager, establish the schedule of decision events, list the underlying assumptions and risks, and detail the resources required (including SMEs) to develop the initial business case. The CM would bring this information together in a project management plan.[5]

An internal governance instrument is required to confirm the arrangements and the release of resources. This could be a committee for complex or high-risk projects,[6] where there is the need for significant engagement with external agencies and departments, or where resources for this phase exceed a given threshold. For example, under the current committee structure, this could be an agenda item for the Capability Planning and Resources Steering Committee (CPRSC). Alternatively, for projects below the above thresholds, approval could be delegated to the chair of an appropriate committee. For instance, the cochairs of the CPRSC (i.e., the chief operating officer and the chief assurance officer) could cosign a minute.

An important additional consideration is determining the approach taken for acquisition and the level of project governance required (see Table 4.2). Complex or high-risk projects require special attention, with an experienced and dedicated team to support them. Evidence provided by the Department suggests that such projects are rare in Home Affairs. Certainly, a functional area might oversee one or two such projects over the life of the capability plan. It is recommended that the Department establishes a dedicated capability centrally, and that the CM augment their team with SMEs from their own functional area. Additionally, we recommend the department accesses and utilises Defence's Smart Buyer decisionmaking framework, to help build

---

[4] The choice of governance model will dictate if, when, and how a particular CM will continue the role as phases change.

[5] See, for example, Australian Government, Department of Defence, 2012a, p. 48.

[6] An example for determining project complexity can be found in Table 4.2.

internal knowledge and consensus on the project, frame the project in such a way as to uncouple some of the complexity, and initiate and establish the relevant supporting documentation.[7] The CM may also choose to engage the central agencies and any other departments or portfolio agencies that might have a relevant interest, both to provide them with early awareness and to allow consideration of issues they raise.

In cases where the CM believes that a project is more straightforward, they would seek committee approval to manage this internally within their area of responsibility. In some cases, the CM may deem it more efficient to combine similar projects into an omnibus project, which incorporates a rolling tranche of subprojects. The CM would seek approval of this through a senior committee (such as the CPRSC). This might be particularly relevant for projects where there are limited (evolutionary) changes in the platform or system that are readily available in the open market (e.g., commercial-off-the-shelf solutions) and little change in the other FIC elements. For example, a capability that requires regular updating of ICT systems. This would simplify the approval process, and allow greater funding certainty.

Initial Business Case Development

Currently, the approach Home Affairs employs to develop business cases for projects is appropriate, and aligns closely with that employed elsewhere in the public sector.[8] However, our interviews with Home Affairs staff and a review of some DIBP business cases indicate an inconsistency in input, both in terms of quality and completeness. There was also the suggestion that the detail expected for initial business cases was. Certainly, the level of detail required of the initial business case should be sufficient to support prioritisation across the program. Home Affairs should seek to simplify initial business case information requirements. At a minimum, the documentation should

- **Establish the context for the project:** This includes an explicit link to the strategic objectives, capability gaps and opportunities, the capability requirement, and implications for taking no action.
- **Summarise the project options:** This includes a description, advantages and disadvantages associated with the option, an FIC analysis, a decision schedule, an annual budget estimate for acquisition and sustainment, and discussion of financial instruments.
- **Summarise interdependencies and interoperability issues:** This includes identifying dependencies between each option and other existing and planning capabilities, future gaps that impact the option, and other demands on the resources required for the operation and sustainment of this capability option.

---

[7] We note that Home Affairs has initiated discussion with Defence on this.

[8] See, for example, Australian Government, Department of Defence, 2012a, p. 55.

- **Summarise internal stakeholder viewpoints:**[9] This includes capturing the perspectives of such key internal stakeholders as Finance Division, People Division, the ICT Division, the operator community, those responsible for acquisition and sustainment, and those working on infrastructure.
- **Outline the engagement strategy:** This includes defining engagement requirements with other departments and agencies that might directly support the acquisition and sustainment of the capability, and the time and nature of engagement with the central agencies.
- **Outline industry capability:** This includes the level of industry support required, the maturity of the marketplace, and strategy for engaging industry (if required).
- **Outline the key risks:** This would include enterprise and project risks, their level, and possible mitigations.
- **Recommend a preferred option:** This includes providing a comparative analysis of project options against capability requirements to establish the preferred option.
- **Summarise the supporting evidence:** This includes providing a description of the evidence and analysis that underpin the options.

A quality assurance process is required once the initial business case has been developed. This would ensure that the business case is of the quality and completeness necessary to allow prioritisation across the program.

Integrated Investment Program

Having developed initial business cases for all approved new projects, the next step is to establish which projects will be developed further, over what time frame, and using which funding instruments.[10] Using the Department and Portfolio finance plans, a determination can be made as to how much funding is available over the forward estimates. Anticipating that the total funding required to support the preferred option for all projects will exceed the available funding, a risk-based mechanism to optimise the program will be necessary. Other constraints, such as workforce number (including skill and competency requirements), infrastructure requirements, and ICT demands would also be included. Critically, the CM represents the projects under them during this process. Further, the approach to optimisation should lead to a negotiated solution that is based on the overall organisational needs, rather than balancing investment across the functional areas.

---

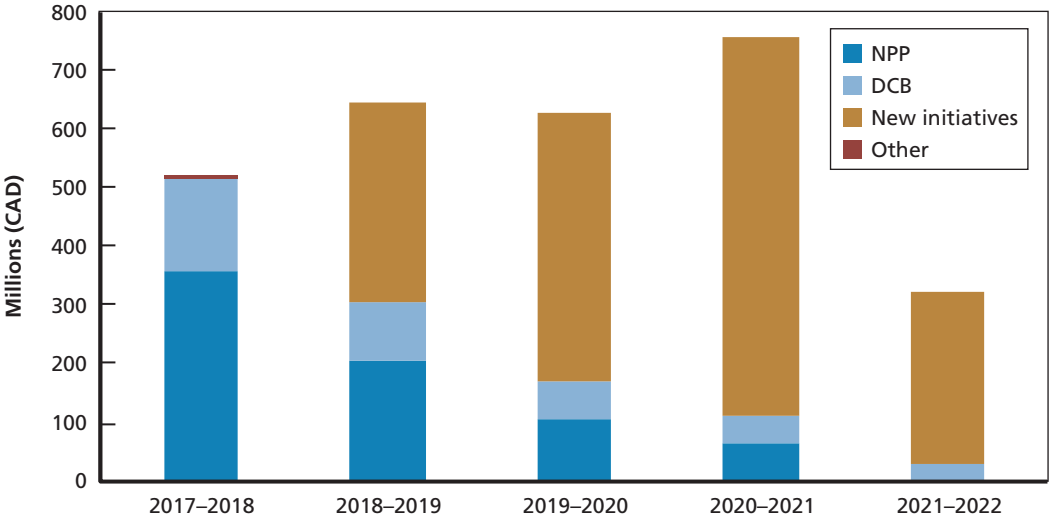
[9] The aim here is not to achieve consensus, but rather to ensure all viewpoints are considered prior to the decision being made.

[10] It is assumed here that while the Portfolio capital budget is approved on a year-by-year basis in response to the government's budget priorities, once a project is approved for funding under this mechanism, it does not need to seek reapproval each year other than by exception.

Specialist tools exist that can undertake such an optimisation; however, in their absence, an iterative process will be necessary. This would commence with a determination of which projects have already been approved in the previous year, are deemed essential, or which are considered unessential. For the years when the major review is occurring, this would include projects that had previously been approved, but where the investment approval has yet to be completed. The remainder, a considerably smaller set, would then be suboptimised to determine an agreed maximal benefit. This might require selection of nonpreferred but lower-cost option to provide better coverage.

The outcome of this is a five-year Home Affairs integrated investment program which would be sent to government for approval. Once approved, it would provide Home Affairs with a level of funding certainty, with which it could develop and deliver the capabilities that the Australian government requires. In effect, it identifies which projects will be supported, the option that is supported, the funding mechanism, the anticipated expenditure over time (see Figure I.1), and the implications for the enabling strategies, such as HR, ICT and RD&I. As shown in Figure I.1, the nature of the expenditure should be captured and should include anticipated future funding wedges for projects that are in the capability plan, but are yet to be initiated. The integrated investment plan should also include the projected sustainment and disposal costs. Otherwise, there is little capacity to understand the feasibility of the strategy-to-capability link. Similar information to that displayed in Figure I.1 should also be shown for staffing, to ensure there is a better understanding of the recruitment, training and reskilling required to meet the capability expectations, as well as to forecast when there will

Figure I.1
2017–2018 Five-Year Investment Plan



SOURCE: Based on data provided by the Department of Home Affairs.

be a need for a surge capability. This will ensure the efficient and targeted use of professional service providers.

I.3 Governance

As noted previously, the Department established a five-year integrated investment plan for FY 2018–2019. However, we observe some issues that suggest the governance of the capability definition phase requires some attention. It was unclear whether dedicated resources were allocated to this phase, though it appears that when this did occur, they were taken from operational funds and might not have been sufficient. We also observe that the investment plan was not adhered to when it came to investment decisions. We cannot definitively explain why this was the case. However, interviewees suggested that these changes may have been due to the establishment of the Department, or because some functional areas made the determination that some of the agreed priorities were not necessary. This emphasises the importance of shared decisionmaking among senior management, appropriate responsibility and accountability for those charged with delivering the capability to the operator community, and an empowered assurance function to ensure that the integrity of the investment program is maintained. This function should not actively participate in the program prioritisation activity, and instead help with facilitation and arbitration. In essence, those responsible for the governance function would provide quality assurance through an audit of the integrated investment program, typically asking similar questions to the capability requirements phase (see Table 4.1).

APPENDIX J

Governance Best Practice

The ability to develop and implement best practices in governance will be key for the successful implementation of an efficient and effective CLMM for Home Affairs. In 2007, the APSC developed a best practice guide for governance for senior public service executives.[1] One of the key observations from the APSC guide was that 'governance can only work if it is part and parcel of the culture of the organisation – it needs to be actively upheld and implemented by every person in the organisation. Everyone must know and act on their responsibilities'.[2] While acknowledging that there is no 'one size fits all' approach to governance, the APSC developed a governance framework based on the principles of good public sector governance. The framework included the following:

- **Accountability:** being answerable for decisions and having meaningful mechanisms in place to ensure the agency adheres to all applicable standards.
- **Transparency and openness:** having clear roles and responsibilities and clear procedures for decisionmaking and exercising power.
- **Integrity:** acting impartially, ethically, and in the interests of the agency, and not misusing information acquired through a position of trust.
- **Stewardship:** using every opportunity to enhance the value of public assets and institutions for which the government has been entrusted to care for.
- **Efficiency:** ensuring the best use of resources to further the aims of the organisation, with a commitment to evidence-based strategies for improvement.
- **Leadership:** achieving an agency-wide commitment to good governance through leadership from the top.

In 2017, UK Treasury published its corporate governance code of best practice.[3] This publication included two additional attributions of good governance, which were

1 Australian Government, 2007.

2 Australian Government, 2007.

3 United Kingdom Government, Her Majesty's Treasury, Cabinet Office, *Corporate Governance in Central Government Departments: Code of Good Practice*, April 2017.

effectiveness (bringing a wide range of relevant experience to bear, including through offering rigorous challenge and scrutinising performance) and **sustainability** (taking a long-term view about what the department is trying to achieve and what it is doing to get there).

In 2005, the U.S. GAO developed a framework for assessing the acquisition function at federal government agencies.[4] This framework identified four interrelated cornerstones that promote an efficient, effective and accountable acquisition function (see Table J.1). The framework further explored these cornerstones in terms of their elements and critical success factors.

CASG, within Defence, has also established common values that underpin their culture and business framework. These values include the following:

- **Professionalism**: striving for excellence in everything we do. We work hard to deliver high quality results, do our job to the best of our ability and take pride in our achievements. We are sensitive to changes in our working environment and are ready to respond. We provide impartial, comprehensive, timely and accurate advice. We constantly seek to improve our work performance.
- **Loyalty:** being committed to each other and to Defence. We serve the government of the day and support our leaders and colleagues to undertake tasks and achieve results in line with government direction. We treat everyone at all levels with respect, care and compassion. We work to uphold the best interests of the Australian people.
- **Integrity:** doing what is right. We behave honestly and ethically, and demonstrate the highest standards of probity in our personal conduct. We act fairly and accept personal responsibility for our decisions and actions. We build trust through productive working relationships. We do not allow mateship to be misused to cover up bad behaviour or bring the organisation into disrepute. Our actions clearly match our words.
- **Courage:** the strength of character to honour our convictions (moral courage) and bravery in the face of personal harm (physical courage). We stand up for what we believe is right and we speak out robustly and openly against what is wrong. We have the courage to accept valid criticism, admit to errors, learn lessons and improve. We give honest feedback on work performance.
- **Innovation:** actively looking for better ways of doing our business. We are open to new ideas and strive to identify and implement better ways of doing business. We are clever and make best use of the resources that we have to do our job. We encourage sensible risk taking, and strive to identify opportunities to eliminate inefficiency and waste.

---

[4] U.S. Government Accountability Office, *Framework for Assessing the Acquisition Function at Federal Agencies*, GAO-05-218G, September 2005.

- **Teamwork:** working together with respect, trust and a sense of collective purpose. We cultivate teamwork through strong, positive leadership and attention to the needs of team members. Teamwork is integral to everything we do, and characterises our working relationships inside Defence and across the whole of government. We foster collaborative workplaces, communicate openly and solve problems in a collegiate manner, share ideas and take advantage of the diversity of our knowledge and experience.'[5]

[5] Australian Government, Department of Defence, 2017b, pp. 7–8.

Table J.1
GAO Cornerstones of Assessing Acquisition

Cornerstone	Elements	Critical Success Factors
Organisational alignment and leadership	Aligning acquisition with agency's missions and needs	• Assuring appropriate placement of the acquisition function • Organising the acquisition function to operate strategically • Clearly defining and integrating roles and responsibilities
	Commitment from leadership	• Clear, strong and ethical executive leadership • Effective communications and continuous improvement
Policies and processes	Planning strategically	• Partnering with internal organisations • Assessing internal requirements and the impact of external events
	Effectively managing the acquisition process	• Empowering crossfunctional teams • Managing and engaging suppliers • Monitoring and providing oversight to achieve desired outcomes • Enabling financial accountability
	Promoting successful outcomes of major projects	• Using sound capital investment strategies • Employing knowledge-based acquisition approaches
Human capital	Valuing and investing in the acquisition workforce	• Commitment to human capital management • Role of the human capital function
	Strategic human capital planning	• Integration and alignment • Data-driven human capital decisions
	Acquiring, developing, and retaining talent	• Targeted investments in people • Human capital approaches tailored to meet organisational needs
	Creating results-oriented organisational cultures	• Empowerment and inclusiveness • Unit and individual performance linked to organisational goals
Knowledge and information management	Identifying data and technology that support acquisition management decisions	• Tracking acquisition data • Translating financial data into meaningful formats • Analysing goods and services spending
	Safeguarding the integrity of operations and data	• Ensuring effective general and application controls • Data stewardship

SOURCE: U.S. Government Accountability Office, 2005.

APPENDIX K

Governance Models Considerations

The following three distinct governance models have been developed, based upon existing practices, each with a decreasing level of centralisation in oversight and management:

- **Centralised governance:** where responsibility for defining and developing the capability is separated from its delivery and sustainment, and provided by two separate entities within the Department.
- **Semicentralised governance:** where the capability is centrally developed, delivered and sustained by a single entity within the Department.
- **Decentralised governance:** where the agencies develop, deliver and sustain their own capabilities.

For each of the models, it is assumed that there will be a committee structure in place to:

- manage performance
- set priorities
- ensure project synchronisation
- approve funding
- provide a mechanism for stopping projects
- provide assistance
- provide advice to government on whether Home Affairs is meeting government guidance, and making the most effective and efficient use of its resources.

For the purpose of this report, we assume that the existing Department committee structures will be able to incorporate the functions of a capability committee and investment committee. The role of the capability committee is as the primary decision-making committee, focused on ensuring key capabilities are managed appropriately and determining resource trade-offs. The investment committee is a subsidiary of the capability committee, and is responsible for overseeing the management and delivery of the integrated investment plan.

A comparison of each model is then made, with accountability determined using a responsible, accountable, consulted, and informed (RACI) framework.[1] We note that the models are described in broad terms to support discussion.

K.1 Centralised Governance Model

The centralised governance model has been derived from the capability development model employed by Defence from 2003 to 2016, where the Capability Development Group was responsible for the capability requirements to investment approval stages of the CLMM, while the Defence Materiel Organisation was responsible for the capability delivery to capability disposal stages.

In the centralised governance model, one entity is responsible for capability requirements, capability definition, and investment approval, while a different entity is responsible for capability delivery, sustainment and disposal. The key attributes of the centralised governance model are provided in Table K.1. Table K.2 outlines which stakeholders are responsible, accountable, consulted and informed within the centralised governance model.

K.2 Semicentralised Governance Model

The semicentralised governance model is a centralised model where the CM defines the requirements and the delivery agent is responsible for the acquisition and through-life support elements of the capability. This model was chosen as a means for ensuring that the authority responsible for acquisition also holds responsibility for the through-life support elements of a capability. The key attributes of the semicentralised governance model are provided in Table K.3. Table K.4 outlines which stakeholders are responsible, accountable, consulted and informed within the semicentralised governance model.

K.3 Decentralised Governance Model

The decentralised governance model is a similar model to that currently employed within the Portfolio. Within the model, each CM is responsible for all stages of the

[1] This framework was chosen as a tool to clarify the roles that each of the key stakeholders would play for each of the models proposed. Within this framework, 'responsible' represents the person who does the work, 'accountable' is the person who must approve the work, 'consulted' are the people who need to give input before the work can be completed, and 'informed' are the people that require updates on progress or decisions.

CLMM, with key decisionmaking taking place within each of the agencies.[2] The key attributes of the decentralised governance model are provided in Table K.5. Table K.6 outlines which stakeholders are responsible, accountable, consulted and informed within the decentralised governance model.

K.4 Model Comparison

Table K.7 provides a comparison between the three governance models. These provide a basis for determining which model suits Home Affairs.

Table K.1
Centralised Governance Model

Role	Description
Capability manager	• Key stakeholder during capability delivery, and closely involved in accepting equipment into service • Shared responsibility during capability operation, sustainment and disposal
Capability development manager	• Allocated funds from a central decisionmaking process for capability requirements, capability definition, and investment approval • Controls the funds for these same stages • Determines requirements in consultation with the CM • Has the ability to adjust requirements in accordance with the needs of each stage the capability development manager is responsible for, in consultation with the CM
Delivery agent	• Allocated funds from a central decisionmaking process for capability delivery, sustainment and disposal • Controls the funds for these same stages • Has the ability to adjust requirements in accordance with the needs of each stage the delivery agent is responsible for, in consultation with the CM
Prioritisation	• Prioritised centrally
Capability committee	• Conducted centrally • Chaired by the secretary
Investment committee	• Conducted centrally • Chaired by at least a deputy secretary
Contestability	• Conducted centrally

[2] Note that in the United Kingdom, the partition is along functional lines (e.g., cyber, counterterrorism, national resilience); see United Kingdom Government, Cabinet Office, 2018a

Table K.2
RACI Matrix for the Centralised Governance Model

	Strategic Planning	Capability Requirements	Capability Definition	Investment Approval	Capability Delivery	Sustain	Dispose
Capability committee	A	A	A	A	A	A	A
Investment committee	R	R	R	R	R	R	R
Capability manager	C	C	C	C	C	R	R
Capability development manager	C	R	R	R	C	C	C
Delivery agent	C	C	C	C	R	R	R
Strategy	R	C	C	C	C	I	I
Contestability	C	R	R	R	R	R	R
Corporate operations	C	C	C	C	C	C	C
Finance	I	C	C	R	R	R	R

NOTE: R = Responsible; A = Accountable; C = Consulted; I = Informed.

Table K.3
Semicentralised Governance Model

Role	Description
Capability manager	• Allocated funds from a central decisionmaking process • Control funds throughout the CLMM • Defines the requirements • Key stakeholder during capability delivery and closely involved in accepting equipment into service
Delivery agent	• Support the CM to define the requirements • Responsible for the capability definition to capability disposal stages of the CLMM
Prioritisation	• Prioritised centrally
Capability committee	• Conducted centrally • Chaired by the secretary
Investment committee	• Conducted centrally • Chaired by a deputy secretary
Contestability	• Conducted centrally

Table K.4
RACI Matrix for the Semicentralised Governance Model

	Strategic Planning	Capability Requirements	Capability Definition	Investment Approval	Capability Delivery	Sustain	Dispose
Capability committee	A	A	A	A	A	A	A
Investment committee	R	R	R	R	R	R	R
Capability manager	C	R	C	C	C	C	C
Delivery agent	C	C	R	R	R	R	R
Strategy	R	C	C	C	I	I	I
Contestability	C	R	R	R	R	R	R
Corporate operations	C	C	C	C	C	C	C
Finance	I	C	C	R	R	R	R

Table K.5
Decentralised Governance Model

Role	Description
Capability manager	• Allocated funds directly from government • Controls funds throughout the CLMM • Controls each stage of the CLMM
Prioritisation	• Prioritised by each CM
Capability committee	• Conducted by each agency • Chaired by head of the responsible agency
Investment committee	• Conducted by each CM • Chaired by at least an assistant secretary or equivalent
Contestability	• Conducted by each CM

Table K.6
RACI Matrix for the Decentralised Governance Model

	Strategic Planning	Capability Requirements	Capability Definition	Investment Approval	Capability Delivery	Sustain	Dispose
Capability committee	A	A	A	A	A	A	A
Investment committee	R	R	R	R	R	R	R
Capability manager	R	R	R	R	R	R	R
Contestability	C	R	R	R	R	R	R
Corporate operations	C	C	C	C	C	C	C
Finance	I	C	C	R	R	R	R

Table K.7
Comparison Between Each Model

Centralised	Semicentralised	Decentralised
Accountability and responsibility for every aspect of the CLMM sits centrally. The CM may see requirements change throughout the process.	Accountability and responsibility for capability requirements is the CM, and all other accountabilities and responsibilities are with a single, central group.	Accountability and responsibility for every aspect of the CLMM sits within one agency.
There can be disconnects between the capability development manager and delivery agent.	It is unlikely for there to be a disconnect between the capability development manager and delivery agent.	This model reinforces the power of the authorities of the agencies and their resource allocation. Oversight may be reduced as all governance takes place within an agency.
Allows more strategic engagement with centralised agencies and government. Allows for omnibus submissions to government.	Allows more strategic engagement with centralised agencies and government. Allows for omnibus submissions to government.	A more direct case can be made to government, based on specific agency requirements. Coordination may be more challenging due to resource limitations within the central agencies.
An efficient use of resources and capability development decisionmaking, with opportunities for rationalisation across capability areas. Opportunities for interoperability considerations between projects, as projects are managed from a single area.	An efficient use of resources and capability development decisionmaking, with opportunities for rationalisation across capability areas. Opportunities for interoperability considerations between projects, as projects are managed from a single area.	This model is a less efficient use of resources. Capabilities are less likely to be interoperable between agencies.

Centralised	Semicentralised	Decentralised
Opportunities for greater buying power and project coordination, as projects are managed from a single group.	Opportunities for greater buying power and project coordination, as projects are managed from a single group.	Lower efficiency, given less coordination between similar projects in different agencies and reduced buying power.
Skill sets can be specialised within capability requirements, contracts and sustainment, allowing for surge capacity on projects if required.	Skill sets can be built within one area, allowing for surge capacity across the program. Skill sets between capability requirements, contracting and sustainment are not easily transferrable.	There will be fewer capability lifecycle experts to address requirements, which could challenge surge capacity and the ability to specialise.
The physical separation of SMEs from capability decisionmakers could deliver less-informed decisions due to reduced familiarity with the detail requirements for each capability.	The physical separation of SMEs from capability decisionmakers could deliver less-informed decisions due to reduced familiarity with the detail requirements for each capability.	There is a greater relationship between the operators and the decisionmakers.
Opportunities for consistent policies across the Portfolio, with projects being managed from a single area.	Opportunities for consistent policies across the Portfolio, with projects being managed from a single area.	Policy can be tailored to the specific needs and authorities of the agency.
Robust prioritisation between projects is needed to ensure that every CM receives the capabilities they need.	Robust prioritisation between projects is needed to ensure that every CM receives the capabilities they need.	Prioritisation can occur in accordance with the needs of the agency, rather than Portfolio priorities.

K.5 Threshold Determination

An example of a framework to determine the implications of the size, risk and complexity of a project is provided in Table K.8. The exact definitions for each category should be developed in consultation with key Home Affairs staff.

Projects that only require a low level of oversight can be rapidly moved through the approval process, with some key decision points not applicable. Projects that require a medium or high level of oversight may need to ensure that they provide decisionmaking bodies with documentation at each decision point. Analysis of projects based upon Table K.8 might be used by Home Affairs to inform the central agencies and government about the level of approval required and the key considerations for each project.

Table K.8
Example of a Framework to Determine Project Size, Risk and Complexity

	High	Medium	Low
Size	• Determine cost range from historic data • Determine longevity range from historic data	• Determine cost range from historic data • Determine longevity range from historic data	• Determine cost range from historic data • Determine longevity range from historic data
Complexity	• FIC not in place • Significant integration required	• Some FIC are in place • Some integration required	• Most FIC are in place, with a robust plan for finalising remaining FIC • Little integration required
Risk	• Major uncertainties remain • No or little prior experience or data	• Some uncertainties remain • Some experience and data exist	• Few uncertainties remain • Significant experience and data exist

APPENDIX L

The Capability Development Function

Having an endorsed approach to undertake capability development represents only part of the solution. What is also required is having the internal capacity to support it. All organisations that we reviewed have such a capability, often characterising it as an enabling capability (see Chapter Three). Further, our interviews with officials from across the Department showed that such a function is critical to the future success of Home Affairs, and that it was currently lacking within the Department. While there will be resource overhead in establishing this function (in addition to the resources required to design and develop the individual capability project proposals), best practices indicate that Home Affairs should establish a dedicated capability development function and provide dedicate resources accordingly.

Given the broad acceptance of this need, the issue is what form it should take, and in particular, the size and skill base required. To come up with a definitive answer to this is problematic on a number of grounds (discussed below). While we can make a definitive recommendation as to the need for Home Affairs to establish and resource a capability development function, we cannot make any firm recommendations regarding the form of that function. However, we will provide some observations based on our review of public sector organisations with similar requirements, since establishing this capability is a necessary early step for the successful implementation of capability development within Home Affairs. We believe these observations can assist the Department in resolving this.

The primary issue is that a definitive response requires agreement on Home Affairs' choices around how it enacts the CLMM and on the governance model that supports it. As indicated earlier, there is some flexibility in the selection of a logic model for the early phases. Further, the nature of the work done within those models, particularly in terms of evidence-building and supporting analysis, has a strong correlation to the composition of the capability development workforce. Finally, and tied to the two previous points, the establishment of the capability development function, along with the body of knowledge, process and tools, will likely incur a significant initial cost. For example, like Defence, Victoria Police employs a scenario-based analytical approach to

assist in capability assessment and prioritisation.[1] This has required significant effort in establishing the basis for this type of analysis, even for an organisation that has a more constrained operational space than Home Affairs.

The other limiting factor that follows from the choice of CLMM is the operating culture within which it is to operate. We note that it is generally the practice for organisations in similar situations to take a rigorous approach to determine staff numbers, using mechanisms such as needs analysis to understand the demands on and flow of workplace requirements. This does provide some useful insights into the broad skills and systems that they might employ. However, observations on such analyses suggest that in public sector environments, legislative, governance, policy, employment practices and other internal process are unique to a workplace, meaning there is limited opportunity to transfer that knowledge to another context. For instance, the number of legislative and financial instruments present within Home Affairs is significantly larger than in most public sector organisations. As a result, a capability development function within Home Affairs might also require access to knowledge and experience associated with this complication. Similarly, while Defence has many similarities to Home Affairs, it operates in an environment that focuses on expenditure. By contrast, Home Affairs collects revenue on behalf of the Australian government at a level second only to the Australian Tax Office.

Finally, there are structural factors. The scrutiny function is crucial. However, the level of assurance and contestability performed, and where this scrutiny function is situated in the organisation, may impact the skills and resources available. Further, the Portfolio's choices around shared services can also affect capability development, given that there is likely to be some level of capability development function resident in the Portfolio agencies in direct support of the capability manager. Portfolio agencies also cover a wide remit. This is likely to affect the scale of embedded operator support. Finally, the Department may choose to have the capability development and acquisition functions colocated. If this were the case, there may be efficiencies from having a larger pool in some key skill areas.

L.1 Domestic Examples

Force Design Division

As a result of the *First Principles Review*, Defence established the FDD within the VCDF Group. Its functions focus both on the design of the current ('test the force in being')[2] and future ('design and guide the development of a balanced and affordable

[1] Victoria Police, 2016, p. 13.

[2] Australian Government, Department of Defence, "Force Design Division," webpage, undated-b.

future force)'[3] Defence capabilities. From a capability development perspective, the FDD's role in the development and testing of capability options at the enterprise level and their smooth transition over time into the Defence force is of particular relevance. These challenges and the FDD's responses to them align closely with the challenges facing Home Affairs as it seeks to take a more strategic and forward-looking perspective, while simultaneously continuing to maintain operational capability to respond to immediate problems. FDD consists of the following three branches:

- Force Options and Plans, which focuses on force options testing, force structure planning, and prioritisation
- Investment Portfolio Management, which focuses on investment management, performance measurement, and governance
- Joint Force Analysis, which focuses on concepts, doctrine, lessons and preparedness.[4]

The Force Options and Plans Branch contains many of the functions Home Affairs requires to enable capability development and inform investment decisions. Advice from within the branch indicates that (as of 24 September 2018) it has 28 substantive staff, comprising nine military officers, 15 APS staff, and four embedded analysts from DST Group.[5] The functions it delivers include the following:

- managing the enterprise-level capability design cycle
- leading the capability assessment program
- supporting integrated investment program decisionmaking
- developing, exploring and assessing capability options
- performing force structure assessments to inform future force design
- analysing, synthesising and prioritising force design outputs
- delivering prioritised and viable portfolio options.[6]

Capability Acquisition and Sustainment

While CASG is focused on the later phases of the capability lifecycle, they have articulated the type of support they provide in advance of the investment decision. They divide this into two broad functions: strategy and concepts, where they are 'supporting needs development, especially technical and commercial factors; developing initial

---

3 Australian Government, Department of Defence, undated-b.

4 Australian Government, Department of Defence, "Force Options and Plans," presentation to the 2017 Force Design Conference, 2017c.

5 The Investment Portfolio Management Branch is of a similar size to Force Options and Planning Branch, and lends support to committees in portfolio governance, coordination and measurement.

6 Australian Government, Department of Defence, 2017c.

project risk profiles and project execution strategies; and coordinating early Industry involvement';[7] and risk mitigation and requirement setting, where they are 'developing an executable, affordable Integrated Project Management Plan; identifying and managing risks to the plan; planning for sustainment and disposal; coordinating Industry engagement; working with the Capability Manager to develop requirements from their needs; managing tendering and tender evaluation; and supporting the development of business cases by Capability Managers'.[8]

Given that this aligns with many of the components of the CLMM proposed here, it is worth considering their model for delivering these functions. We note that CASG has established six functional centres of expertise, of which the following three are particularly relevant to capability development:

- program management, which includes coordinating FIC, independent assurance, and a standardised approach to program management
- engineering and technical, which includes planning, requirements analysis, and definition activities in support of acquisition and sustainment
- decision support, which includes reporting of performance, provides stewardship of management support systems and decisionmaking tools, and oversight of internal information management.[9]

Victoria Police

Victoria Police has made a significant investment in capability planning, with the view that it will reshape how it operates, and thus improve the support it provides to the Victoria community. Under their approach, Victoria Police is seeking to establish a system that provides a focus on the integration between policies, legislation and capabilities; places the development and sustainment of capabilities on an equal footing; aligns capability needs with current and future demands; encourages an environment of innovation and continuous improvement; seeks out opportunities to streamline internal process; and aligns strategy, business planning and policy.[10] While it does not explicitly state the functions it is developing to enable this, it does indicate some drivers, including[11]

- assessing capability maturity to identify where resources can be best used to deliver timely and high-quality services

---

7 Australian Government, Department of Defence, 2017b.

8 Australian Government, Department of Defence, 2017b.

9 Australian Government, Department of Defence, 2017b.

10 Victoria Police, 2016, p. 15.

11 Victoria Police, 2016, p. 5.

- helping to better respond to new and emerging issues by assessing the resources, skills and equipment
- prioritising and demonstrating the need for incremental investment by clearly linking projects to the maintenance and maturation of existing capability
- embedding a capability lifecycle approach within internal planning processes
- identifying common issues and developing a more coordinated approach across capabilities to realise better outcomes in terms of value for money and strategic public value.

Victoria Police noted that its capability development team comprises approximately 25 members with representation from both operators (generally late-career police officers) and civilians with skills in strategic thinking, policy development, research and analysis, proposal writing, or some combination of those. It noted that it has been a deliberate decision to build an internal capability, rather than seek external service providers, in order to maintain stability and knowledge.

L.2 International Examples

U.S. Department of Homeland Security

Staff within the JRC support its mission to build a cross-DHS collaborative environment to validate and prioritise operational requirements for all major acquisitions, and to ensure that objective, analytical rigour supports those requirements. As a centralising and coordinating entity that supports capability development, this represents an example of the roles and functions Home Affairs might need to build to support capability development. The JRC workforce supports the following missions:[12]

- implementation and execution of the JRIMS process, which includes coordinating submission of documents
- in terms of process, performing initial reviews of the documents to assess quality and categorisation purposes, and providing analysis and coordination to support adjudication by council members and to validate recommendation
- provision of training to component staff on the requirements process, particularly in terms of providing standardised and authoritative training on the JRIMS
- analysis of joint capabilities and requirements; until recently, this was through CGA, which assesses capability gaps from across DHS in order to create a prioritised list of unmet capabilities for the department; JAR, which assesses existing programs, in both development and sustainment, in order to create an investment

[12] Vasseur et al., 2018.

decision support tool; and through facilitating a stakeholder working group that develops the approach and assessment criteria used by CGA and JAR (recently, the JRC established the Capability Gap Register, which incorporates the CGA and part the JAR)

- requirements outreach, including advising various DHS agency requirements staff during the capability development process; attending enterprise-wide forums related to requirements development, including acquisition review teams; policy development working groups; and DHS research and development integrated product teams.

Glossary

This report employs and, in many cases has developed, definitions for key terms. These are defined in the table below.

balance of investment	Evaluating the requirements of the organisation in terms of cost, capability and schedule, and optimising these based upon applicable constraints.
capability	The capacity and intent to achieve and sustain a desired effect or output to meet one or more strategic objectives.
capability-based planning	Planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances, while working within an economic framework.
capability definition	The third phase of the CLMM. This phase encompasses the establishment of capability proposals, the development and exploration of options for addressing the capability requirements, and the development of business cases to support prioritisation across a multiyear integrated investment program.
capability design	Develops the acquisition strategy for capability development by establishing the medium-term investment program, from which individual capability projects establish their business cases for approval. This represents phases 3 (capability definition) and 4 (investment approval) of the CLMM.
capability development	The ability to develop and maintain the most operationally effective and cost-efficient mix of capabilities required to achieve the government's strategic objectives.
capability identification	Takes strategic guidance and translates it into operational tasks and then capability needs. Prioritised gaps are identified and capability options are explored to establish a 10-year capability plan. This represents phases 1 (strategic planning) and 2 (capability requirements) of the CLMM.
capability lifecycle	The phases through which a capability system passes through from the identification of the need to its disposal.
capability requirements	The second phase of the CLMM. This is the point at which high-level capability gaps are identified, prioritised and endorsed. Capability proposals (incorporating capability needs statements and indicative budget provisions) are developed, and likely funding mechanisms identified, either externally via funding instruments such as an NPP, or internally through the DCB.

key enablers	The enterprise-level functions which support and contribute to the efficiency, effectiveness and sustainment of the operational functions.
fundamental inputs to capability	Fundamental inputs to capability is the standard list for consideration of what is required to generate capability. It allows for a comprehensive analysis and planning of capability, and the ability to focus attention on the combination and integration of the inputs, rather than on the individual inputs separately.
investment approval	The fourth phase of the CLMM. This phase transforms prioritised capability options into well-defined and costed solutions incorporating all FIC, and that include whole-of-life workforce numbers and budgetary provisions to acquire, operate and sustain the capability solution.
Portfolio	The Home Affairs Portfolio consists of the Department of Home Affairs, as well as a number of statutory agencies which may be governed under differing legislative arrangements and may utilise differing funding instruments. The five agencies within the Portfolio are Australian Border Force (ABF), Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), Australian Security Intelligence Organisation (ASIO) and Australian Transaction Reports and Analysis Centre (AUSTRAC).
strategic planning	The first phase of the CLMM. This phase focuses on strategy and its role in informing and shaping capability development. It provides a risk-based view of the Department's present and future direction to inform forward planning of investment across the life of a capability, including acquisition, operations, sustainment and disposal.

Bibliography

Anderson, Sharon, "Delivering Decisive Understanding to the Commander," *CHIPS*, April–June 2016. As of 3 May 2019:
https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=7899

Australian Border Force, *ABF 2020*, Australian 2016. As of 3 May 2019:
https://www.homeaffairs.gov.au/commitments/files/abf-2020.pdf

Australian Government, *Building Better Governance*, Australian Public Service Commission, 2007. As of 3 May 2019:
https://www.apsc.gov.au/building-better-governance

Australian Government, *National Security Science and Innovation Strategy*, Department of the Prime Minister and Cabinet, 2009. As of 3 May 2019:
https://www.dst.defence.gov.au/sites/default/files/basic_pages/documents/NSSIS-strategy.pdf

Australian Government, *Policing for a Safer Australia: Strategy for Future Capability*, Australian Federal Police, March 2017. As of 3 May 2019:
https://www.afp.gov.au/sites/default/files/PDF/strategy-for-future-capability.pdf

Australian Government, *National Security Science and Technology Policy and Priorities*, Defence Science and Technology, 2018. As of 3 May 2019:
https://www.dst.defence.gov.au/sites/default/files/research_facilities/documents/NS-S%26T-policy-and-priorities.PDF

Australian Government, Department of Defence, *Capability Life Cycle Detailed Design: Executive Summary*, undated-a. As of 3 May 2019:
http://www.defence.gov.au/publications/docs/Capability-Life-Cycle-Detailed-Design.pdf

Australian Government, Department of Defence, "Force Design Division," webpage, undated-b. As of 3 May 2019:
http://www.defence.gov.au/VCDF/FD/

Australian Government, Department of Defence, *The Simplified Defence Business Model*, undated-c. As of 3 May 2019:
http://www.defence.gov.au/Publications/SimplifiedDefenceBusinessModel.pdf

Australian Government, Department of Defence, *Going to the Next Level: The Report of the Defence Procurement and Sustainment Review*, 2008. As of 3 May 2019:
http://www.defence.gov.au/publications/mortimerReview.pdf

Australian Government, Department of Defence, *Defence Capability Development Handbook 2012*, 2012a. As of 3 May 2019:
http://www.defence.gov.au/publications/DefenceCapabilityDevelopmentHandbook2012.pdf

Australian Government, Department of Defence, *Defence Capability Plan: Public Version 2012*, 2012b. As of 3 May 2019:
http://www.defence.gov.au/publications/CapabilityPlan2012.pdf

Australian Government, Department of Defence, *First Principles Review: Creating One Defence*, 2015. As of 3 May 2019:
http://www.defence.gov.au/publications/reviews/firstprinciples/Docs/FirstPrinciplesReviewB.pdf

Australian Government, Department of Defence, *2016 Defence White Paper*, 2016a. As of 3 May 2019:
http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf

Australian Government, Department of Defence, *2016 Integrated Investment Program*, 2016b. As of 3 May 2019:
http://www.defence.gov.au/whitepaper/Docs/2016-Defence-Integrated-Investment-Program.pdf

Australian Government, Department of Defence, *Defence Industry Policy Statement*, 2016c. As of 3 May 2019:
http://www.defence.gov.au/whitepaper/docs/2016-defence-industry-policy-statement.pdf

Australian Government, Department of Defence, "The New Capability Life Cycle Has Commenced," *CASG Bulletin*, June 2016d. As of 3 May 2019:
http://www.defence.gov.au/casg/NewsMedia/DMOBulletin/new_clc

Australian Government, Department of Defence, "Smart Buyer," *CASG Bulletin*, June 2016e. As of 8 May 2019:
http://www.defence.gov.au/CASG/NewsMedia/DMOBulletin/smart_buyer

Australian Government, Department of Defence, *Annual Report 16–17*, 2017a. As of 3 May 2019:
http://www.defence.gov.au/annualreports/16-17/downloads/dar_2016-17_complete.pdf

Australian Government, Department of Defence, *The CASG Business Framework*, 2017b. As of 3 May 2019:
http://www.defence.gov.au/casg/Multimedia/CASG%20Business%20Framework.pdf

Australian Government, Department of Defence, *Force Options and Plans*, presentation to the Force Design Conference, 2017c. As of 3 May 2019:
https://www.unsw.adfa.edu.au/conferences/sites/conferences/files/uploads/user50/DG-FOAP-Branch-Presentation-to-FD-Conerence-10oct2017.pdf

Australian Government, Department of Defence, *2018–19 Defence Corporate Plan*, 2018. As of 3 May 2019:
http://defence.gov.au/publications/Docs/2018-19_Defence_Corporate_Plan.pdf

Australian Government, Department of Finance, *Public Governance, Performance and Accountability Act 2013*, 2013. As of 3 May 2019:
https://www.finance.gov.au/resource-management/pgpa-act/

Australian Government, Department of Finance, *Implementing the Commonwealth Risk Management Policy – Guidance*, Resource Management Guide 211, 2016a. As of 3 May 2019:
https://www.finance.gov.au/sites/default/files/implementing-the-rm-policy.PDF

Australian Government, Department of Finance, *Resource Management Guide No. 130: Overview of the Enhanced Commonwealth Performance Framework*, July 2016b. As of 3 May 2019:
https://www.finance.gov.au/sites/default/files/rmg-130-overview-of-the-enhanced-commonwealth-performance-framework_0.pdf

Australian Government, Department of Finance, *Commonwealth Procurement Rules: Achieving Value for Money*, 1 January 2018. As of 8 May 2019:
https://www.finance.gov.au/sites/default/files/commonwealth-procurement-rules-1-jan-18.pdf

Australian Government, Department of Home Affairs, "Factsheet: Capital Costing," fact sheet, internal document, undated.

Australian Government, Department of Home Affairs, *Blueprint for Home Affairs*, 2018a. As of 8 May 2019:
https://www.homeaffairs.gov.au/commitments/files/blueprint-for-home-affairs.pdf

Australian Government, Department of Home Affairs, *Corporate Plan 2018–19*, 2018b. As of 8 May 2019:
https://www.homeaffairs.gov.au/commitments/files/corporate-plan-2018-19.pdf

Australian Government, Department of Home Affairs, *A Strategy-Led Approach to Portfolio Capability Investment: Draft,* internal document, 2018c.

Australian Government, Department of Home Affairs, *Portfolio Budget Statement 2018–19 Budget Related Paper No. 1.10 – Home Affairs*, 2018d. As of 3 May 2019:
https://www.homeaffairs.gov.au/reports-and-pubs/Budgets/2018-19-full.pdf

Australian Government, Department of Home Affairs, "Project Management Framework 'At a Glance,'" version 4.40, internal document, 2018e.

Australian Government, Department of Home Affairs, *Terms of Reference – Home Affairs and ABF Capability Review (Draft)*, unpublished draft report, 2018f.

Australian Government, Department of Home Affairs *Business Case Template*, version 3.5, internal document, 2018g.

Australian Government, Department of Immigration and Border Protection, *Strategy 2020*, 2015. As of 8 May 2019:
https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/strategy-2020.pdf

Australian Government, Department of Immigration and Border Protection, *Technology Review*, internal document, 2016.

Australian Government, Department of Immigration and Border Protection, *2017–18 Five Year Investment Budget*, Capability Planning and Resources Committee: Agenda Item 3 Attachment F, 29 August 2017a.

Australian Government, Department of Immigration and Border Protection, *Capability Management*, unpublished presentation, 2017b.

Australian Government, Department of Immigration and Border Protection, *Corporate Plan 2017–18*, 2017c. As of 8 May 2019:
https://www.homeaffairs.gov.au/ReportsandPublications/Documents/corporate-plans/corporate-plan-2017-18.pdf

Australian Government, Department of Immigration and Border Protection, *Technology Strategy 2020*, 2017d. As of 8 May 2019:
https://www.homeaffairs.gov.au/commitments/files/technology-strategy-2020.pdf

Australian Government, Department of Infrastructure and Regional Development, *Office of Transport Security: Our Strategy 2017–2020* (INFRA3227, May 2017), 2017a.

Australian Government, Department of Infrastructure and Regional Development, *Transport Security Outlook to 2025*, 2017b. As of 8 May 2019:
https://infrastructure.gov.au/security/files/Transport_Security_Outlook_2025-Security_Environment_Review.pdf

Australian Government, Department of the Prime Minister and Cabinet, *Defence Procurement Review 2003*, 15 August 2003. As of 3 May 2019:
http://www.defence.gov.au/publications/dpr180903.pdf

Australian Government, Office of National Intelligence, "Overview," webpage, undated. As of 3 May 2019:
https://www.oni.gov.au/overview

Australian National Audit Office, "The Management of Risk by Public Sector Entities," 15 August 2017. As of 8 May 2019:
https://www.anao.gov.au/work/performance-audit/management-risk-public-sector-entities

Australian National Audit Office, "Efficiency Through Contestability Programme," webpage, 20 May 2018a. As of 8 May 2019:
https://www.anao.gov.au/work/performance-audit/efficiency-through-contestability-program

Australian National Audit Office, *The Integration of the Department of Immigration and Border Protection and the Australian Customs and Border Protection Service*, 6 June 2018b. As of 8 May 2019:
https://www.anao.gov.au/work/performance-audit/integration-department-immigration-and-border-protection-and-australian-customs-and-border

Brangwin, Nicole, Nathan Church, Steve Dyer, and David Watt, *Defending Australia: A History of Australia's Defence White Papers*, Australian Parliamentary Library, 20 August 2015. As of 8 May 2019:
https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust

Burgess, Richard R., "Minotaur Mission System to Be Added to P-8 in Increment 3 Upgrade," *Seapower*, 5 April 2017. As of 8 May 2019:
http://seapowermagazine.org/stories/20170404-p8.html

Business Architecture Guild, *A Guide to the Business Architecture Body of Knowledge® (BIZBOK Guide)*, version 6.5, 2018. As of 8 May 2019:
https://cdn.ymaws.com/www.businessarchitectureguild.org/resource/resmgr/BIZBOK_6_5/BIZBOK_Guide_v6.5_Part1.pdf

Carr, Lee, Kristen Lambrecht, Scott Shaw, Greg Whittier, and Catherine Warner, *Unmanned Aerial Vehicle Operational Test and Evaluation Lessons Learned*, Institute for Defense Analyses, P-3821, December 2003. As of 16 October 2018:
https://www.dtic.mil/dtic/tr/fulltext/u2/a424895.pdf

Caudle, Sharon, "Homeland Security Capabilities-Based Planning: Lessons from the Defense Community," *Homeland Security Affairs*, Vol. 1, No. 2, August 2005.

Cook, Cynthia R., Emma Westerman, Megan McKernan, Badreddine Ahtchi, Gordon T. Lee, Jenny Oberholtzer, Douglas Shontz, and Jerry Sollinger, *Contestability Frameworks: An International Horizon Scan*, Santa Monica, Calif.: RAND Corporation, RR-1372-AUS, 2016. As of 3 May 2019:
https://www.rand.org/pubs/research_reports/RR1372.html

Cruikshank, Iain J., "Why The Army's New Palantir Contract Won't Fix Battlefield Intelligence," *Task & Purpose*, 8 August 2018. As of 9 December 2018:
https://taskandpurpose.com/army-palantir-contract-problems/

Data Visualization Catalogue, "Sunburst Diagram," webpage, undated. As of 7 May 2019: https://datavizcatalogue.com/methods/sunburst_diagram.html

Davis, Paul K., *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation*, Santa Monica, Calif.: RAND Corporation, MR-1513-OSD, 2002. As of 8 May 2019: https://www.rand.org/pubs/monograph_reports/MR1513.html

Defense Acquisition University, *Defense Acquisition Guidebook*, U.S. Department of Defense, undated-a. As of 8 May 2019: https://www.dau.mil/tools/dag

Defense Acquisition University, "DOTmLPF-P Analysis," *Acquipedia*, undated-b. As of 3 May 2019: https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=d11b6afa-a16e-43cc-b3bb-ff8c9eb3e6f2

De Spiegeleire, Stephan, "Ten Trends in Capability Planning for Defence and Security," *RUSI Journal*, Vol. 156, No. 5, 2011, pp. 20–28.

Dutton, Peter, "Address to the National Press Club of Australia, Canberra," speech delivered at the National Press Club, 21 February 2018. As of 3 May 2019: http://minister.homeaffairs.gov.au/peterdutton/Pages/Address-to-the-National-Press-Club-of-Australia.aspx

Edwards, Peter, "Defence White Papers After 40 Years," Australian Strategic Policy Institute, 9 March 2016. As of 3 May 2019: https://www.aspistrategist.org.au/defence-white-papers-at-40/

Erwin, Mark, "Airborne Solutions for Maritime Border Security Operations: Minotaur Mission Management System," briefing delivered to U.S. Customs and Border Protection, August 2017.

Gerstein, Daniel M., Karen Edwards, Julie Newell, and Dulani Woods, *Looking to the Future of the Department of Immigration and Border Protection (DIBP): Assessment of the Consolidation of the Australian Customs and Border Protection Service (ACBPS) and the DIBP (2016–2017)*, Santa Monica, Calif.: RAND Corporation, RR-2262-AUS, 2017. As of 3 May 2019: https://www.rand.org/pubs/research_reports/RR2262.html

Goodwin, Paul, and George Wright, *Decision Analysis for Management Judgement*, 2nd ed., John Wiley and Sons: Chichester, UK, 1998.

International Organization for Standardization, "Asset Management—Overview, Principles and Technology," ISO 55000:2014(en), 2014. As of 3 May 2019: https://www.iso.org/obp/ui/#iso:std:iso:55000:ed-1:v2:en

Jaiswal, N. K., *Military Operations Research: Quantitative Decision Making*, Springer: New York, 1997.

Judson, Jen, "The Army Turns to a Former Legal Opponent to Fix Its Intel Analysis System," *C4ISRNet*, 9 March 2018. As of 3 May 2019: https://www.c4isrnet.com/land/2018/03/09/army-awards-contract-to-buy-commercial-solutions-to-fix-troubled-intel-analysis-framework/

Koscak, Paul, "Innovative Tech Helps AMO Combat Smugglers," U.S. Department of Homeland Security, Customs and Border Protection, undated. As of 5 September 2018: https://www.cbp.gov/frontline/air-and-marine-operations-minotaur

Office of the Undersecretary of Defense (Acquisitions, Technology, and Logistics), Acquisitions Resources Analysis, Property and Equipment Policy Office, "Frequently Asked Questions," webpage, undated. As of 13 September 2018:
https://www.acq.osd.mil/pepolicy/general/faq.html#top

The Open Group, *Open Group Guide: Business Capabilities*, G161, 2016. As of 3 May 2019:
https://publications.opengroup.org/g161

Organisation for Economic Co-operation and Development, "The UK's National Risk Assessment (NRA)," website, undated. As of 3 May 2019:
https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/page/theuksnationalriskassessmentnra.htm

Parliament of Australia, *Legal and Constitutional Affairs Legislation Committee: Estimates, Department of Home Affairs*, 26 February 2018. As of 8 May 2019:
http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22committees%2Festimate%2F2c68087e-f913-401c-88da-f76e4cc7f2fc%2F0002%22

State Government of Victoria State Services Authority, *Inquiry into the Command, Management and Functions of the Senior Structure of Victoria Police*, 2011. As of 3 May 2019:
https://www.parliament.vic.gov.au/file_uploads/InquiryCommandManagementFunctionsVicPolice2012_DNVV27vr.pdf

Technical Cooperation Program, "Guide to Capability-Based Planning," 2004. As of 3 May 2019:
https://www.acq.osd.mil/ttcp/reference/docs/JSA-TP-3-CBP-Paper-Final.doc

Thaler, David E., *Strategies to Tasks: A Framework for Linking Means and Ends*, Santa Monica, Calif.: RAND Corporation, MR-300-PAF, 1993. As of 3 May 2019:
https://www.rand.org/pubs/monograph_reports/MR300.html

Thirtle, Michael R., Robert V. Johnson, and John L. Birkler, *The Predator ACTD: A Case Study for Transition Planning to the Formal Acquisition Process*, Santa Monica, Calif.: RAND Corporation, MR-899-OSD. As of 3 May 2019:
https://www.rand.org/pubs/monograph_reports/MR899.html

United Kingdom Government, "Integrating the Science and Technology Support for the UK's Defence and Security," webpage, 24 January 2017. As of 3 May 2019:
https://www.gov.uk/government/news/integrating-the-science-and-technology-support-for-the-uks-defence-and-security

United Kingdom Government, "Centre for Applied Science and Technology (CAST) Becomes Part of Dstl," webpage, 24 April 2018a. As of 3 May 2019:
https://www.gov.uk/government/news/centre-for-applied-science-and-technology-cast-becomes-part-of-dstl

United Kingdom Government, *Defence Science and Technology Laboratory Annual Report and Accounts 2017 to 2018*, Defence Science and Technology Laboratory, 18 July 2018b. As of 3 May 2019:
https://www.gov.uk/government/publications/defence-science-and-technology-laboratory-annual-report-and-accounts-2017-to-2018

United Kingdom Government, Cabinet Office, "Guidance Risk Assessment: How the Risk of Emergencies in the UK Is Assessed," webpage, 20 February 2013. As of 3 May 2019:
https://www.gov.uk/guidance/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed

United Kingdom Government, Cabinet Office, *National Security Capability Review*, March 2018a. As of 3 May 2019:
https://www.gov.uk/government/publications/national-security-capability-review-nscr

United Kingdom Government, Cabinet Office, "Guidance: Preparation and Planning for Emergencies," 30 May 2018b. As of 3 May 2019:
https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-the-capabilities-programme

United Kingdom Government, Cabinet Office, "Resilience Capabilities Programme Sunburst Policy Insights (Annex 2)," unpublished presentation, 2018c.

United Kingdom Government, Cabinet Office, "Resilience Capabilities Programme Sunburst Science (Annex 1)," unpublished presentation, 2018d.

United Kingdom Government, Cabinet Office, "Resilience Capabilities Programme Understanding Capability (Annex 5)," unpublished presentation, 2018e.

United Kingdom Government, Her Majesty's Treasury, Cabinet Office, *Corporate Governance in Central Government Departments: Code of Good Practice*, April 2017. As of 3 May 2019:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609903/PU2077_code_of_practice_2017.pdf

United Kingdom Government, Home Office, "Transparency Data: Senior Staff Salary and Structure Information for Home Office: March 2016," webpage, last updated 2 March 2018. As of 3 May 2019:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/654861/20160331_-_Organogram_Data_-_HomeOffice_-senior.csv/preview

United Kingdom Government, Home Office Science Advisory Council, "Minute of the Home Office Science Advisory Council," 28 September 2017. As of 3 May 2019:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/681044/Minute_of_HOSAC_28_09_2017_pub_2.pdf

United Kingdom Government, Ministry of Defence, "Defence Lines of Development Analysis with MODAF," 2009. As of 3 May 2019:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/36720/20090210_MODAFDLODAnalysis_V1_0_U.pdf

U.S. Coast Guard, "Minotaur Mission System," webpage, undated. As of 3 May 2019:
https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-Acquisitions-CG-9/Programs/Air-Programs/Minotaur-Mission-System/

U.S. Coast Guard, Acquisition Directorate, "Minotaur Mission System," fact sheet, April 2018. As of 3 May 2019:
https://www.dcms.uscg.mil/Portals/10/CG-9/Acquisition%20PDFs/Factsheets/Minotaur%20Mission%20system.pdf?ver=2018-04-06-101521-377

U.S. Department of Homeland Security, *Developing Operational Requirements: A Guide to the Cost-Effective and Efficient Communication of Needs*, version 2.0, November 2008.

U.S. Department of Homeland Security, *DHS Acquisition Instruction / Guidebook 102-01-001, Revision 1*, 2016.

U.S. Department of Homeland Security, "JRC Briefing," Joint Requirements Council, September 2018.

U.S. Department of Homeland Security, Management Directorate, *Instruction Manual 262-12-001-01, DHS Lexicon Terms and Definitions: 2017 Edition, Revision 2*, Washington, D.C., October 16, 2017.

U.S. Government Accountability Office, *Framework for Assessing the Acquisition Function at Federal Agencies*, GAO-05-218G, September 2005.

U.S. Government Accountability Office, *Defense Acquisitions: DOD's Requirements Determination Process Has Not Been Effective in Prioritizing Joint Capabilities*, report to the Committee on Armed Services, U.S. Senate, Washington, D.C., GAO-08-1060, September 2008.

U.S. Government Accountability Office, *Homeland Security Acquisitions: Joint Requirements Council's Initial Approach Is Generally Sound and It Is Developing a Process to Inform Investment Priorities*, report to Congressional Requesters, Washington, D.C., GAO-17-171, October 2016.

U.S. Government Accountability Office, *Homeland Security Acquisitions: Earlier Requirements Definition and Clear Documentation of Key Decisions Could Facilitate Ongoing Progress*, report to Congressional Committees, Washington, D.C., GAO-17-346SP, April 2017.

U.S. Government Accountability Office, *DHS Acquisitions: Additional Practices Could Help Components Better Develop Operational Requirements,* report to Congressional Requesters, GAO-18-550, August 2018.

van Asselt, Marjolein B. A., Susan A. van 't Klooster, Phillip W. F.van Notten, and Livia A. Smits, *Foresight in Action: Developing Policy-Oriented Scenarios*, Routledge: London, 2010.

Vance, Ashlee, and Brad Stone, "Palantir, the War on Terror's Secret Weapon," *Bloomberg Businessweek,* 22 November 2011. As of 3 May 2019:
http://www.bloomberg.com/bw/magazine/palantir-the-vanguard-of-cyberterror-security-11222011.html#p1

Vasseur, Michael, Dwayne M. Butler, Brandon Crosby, Benjamin N. Harris, and Christopher Scott Adams, *An Assessment of the Joint Requirements Council's (JRC) Organization and Staffing*, Santa Monica, Calif.: RAND Corporation, RR-2473-DHS, 2018. As of 3 May 2019:
https://www.rand.org/pubs/research_reports/RR2473.html

Victoria Police, *Victoria Police Blue Paper: A Vision for Victoria Police in 2025*, State of Victoria, Australia, 2014. As of 3 May 2019:
http://www.police.vic.gov.au/content.asp?Document_ID=42063

Victoria Police, *Victoria Police Capability Plan 2016–2025: Capability Framework*, State of Victoria, Australia, September 2016. As of 3 May 2019:
http://www.police.vic.gov.au/content.asp?a=internetBridgingPage&Media_ID=120708

Victoria Police, *Victoria Police Capability Plan 2016–2025: Annual Plan 2018–2019*, State of Victoria, Australia, July 2018. As of 3 May 2019:
https://www.police.vic.gov.au/content.asp?a=internetBridgingPage&Media_ID=141933

White, Hugh, "Strategic Interests in Australian Defence Policy: Some Historical and Methodological Reflections," *Security Challenges*, Vol. 4, No. 2, Winter 2008, pp. 63–79.

Whittle, Richard, *Predator: The Secret Origins of the Drone Revolution,* New York: Henry Holt and Company, 2014.

Wong, Jonathan, *Balancing Immediate and Long-Term Defense Investments*, dissertation, Santa Monica, Calif.: The Frederick S. Pardee RAND Graduate School, RGSD-378, 2016. As of 3 May 2019:
https://www.rand.org/pubs/rgs_dissertations/RGSD378.html

Yue, Yi, and Michael Henshaw, "An Holistic View of UK Military Capability Development," *Defense & Security Analysis,* Vol. 25, No. 1, March 2009, pp. 53–67.