Australian Government

Australian Security Intelligence Organisation

ASIO Annual Report 2020–21

ASIO

Securing Australia—protecting its people

Aids to access

ISSN 0815–4562 (print)
ISSN 2204–4213 (online)

Ownership of intellectual property rights in this publication

Creative Commons licence

Commonwealth Coat of Arms

The Commonwealth Coat of Arms is used in accord with the April 2014 *Commonwealth Coat of Arms: information and guidelines*, published by the Department of the Prime Minister and Cabinet and available online (http://www.pmc.gov.au/sites/default/files/publications/Commonwealth_Coat_of_Arms_Information_and_Guidelines.pdf).

Report a threat

National Security Hotline 1800 123 400
hotline@nationalsecurity.gov.au

About this report

This report has been prepared in accordance with the provisions of the *Public Governance Performance and Accountability Act 2013* (PGPA Act), the Public Governance, Performance and Accountability Rule 2014 (PGPA Rule) and the Department of Finance Resource Management Guide Number 135.

Location of this annual report

Further information about ASIO and an online version of this report are available on the ASIO website. The direct address to view this annual report is www.asio.gov.au/asio-report-parliament. The annual report can also be viewed at www.transparency.gov.au.

Contact us

We welcome feedback on our annual report from any of our readers.

Phone

General inquiries	1800 020 648
ASIO Outreach inquiries	02 6234 1688
Media inquiries	02 6249 8381
Recruitment inquiries	02 6257 4916

Email

media@asio.gov.au

Post

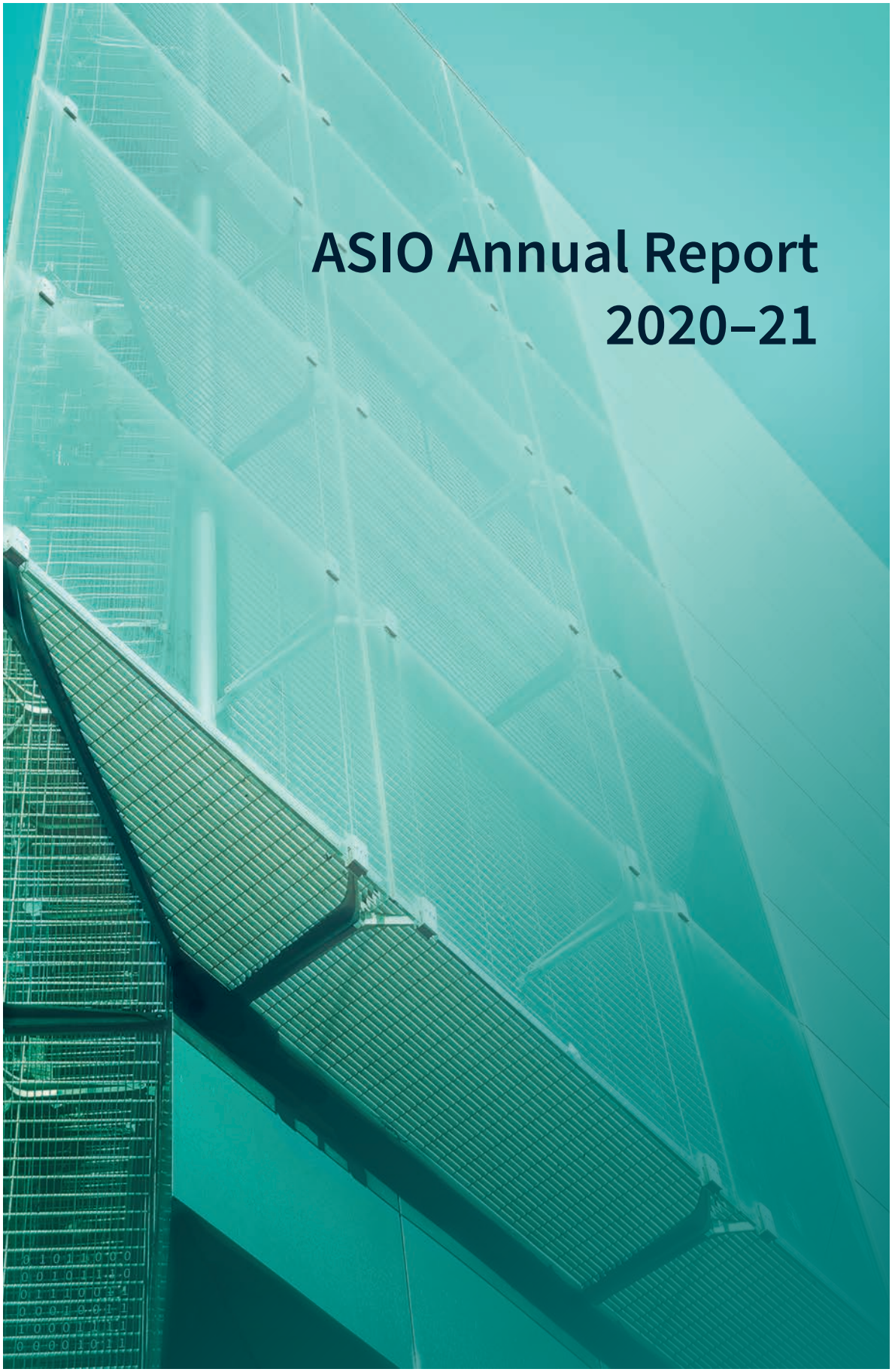
GPO Box 2176, Canberra ACT 2601

State and territory offices

Call 13ASIO (132746)

Acknowledgement of Country

ASIO acknowledges the traditional owners and custodians of country throughout Australia, and acknowledges their continuing connection to land, sea and community. We pay our respects to the people, the cultures and elders past, present and emerging. We also acknowledge the contributions of our Aboriginal and Torres Strait Islander employees in support of our mission.



ASIO Annual Report 2020–21

Australian Government
Australian Security Intelligence Organisation

Director-General of Security

13th September 2021
Ref: A2021956

The Hon. Karen Andrews, MP
Minister for Home Affairs
Parliament House
CANBERRA ACT 2600

Dear Minister,

ASIO Annual Report 2020-21

In accordance with section 46 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), I am pleased to present to you the Australian Security Intelligence Organisation's (ASIO) annual report for 2020-21.

This report contains information required by the *PGPA Rule 2014* and section 94 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). In order to ensure compliance with the Determination made by the Minister for Finance under section 105D of the PGPA Act, the statements required under subsection 94(2A) of the ASIO Act relating to special intelligence operations, special powers under warrant and telecommunications data authorisations have been removed from the annual report tabled in the Parliament in order to avoid prejudice to ASIO's activities. These statements will be separately provided to you and, as required by the ASIO Act, to the Leader of the Opposition. The statement relating to telecommunications data authorisations will also be provided to the Parliamentary Joint Committee on Intelligence and Security.

As required by subsection 17AG(2) of the PGPA Rule, I certify that fraud risk assessments and control plans have been prepared for ASIO; that we have appropriate mechanisms in place for preventing, investigating, detecting and reporting incidents of fraud; and that all reasonable measures have been taken to deal appropriately with fraud.

Yours sincerely,

Mike Burgess

GPO Box 2176 Canberra City ACT 2601

Contents

Securing Australia—protecting its people

1

1

Director-General's review

Director-General's review

Introduction

ASIO is Australia's security service. Every day, across Australia and in select locations around the world, ASIO officers do extraordinary things. They do not do them for recognition, status or accolades. They do them because they believe in ASIO's purpose: to protect Australia and Australians from threats to their security.

Our people are mission-focused, innovative, creative and diverse.

And they make a difference.

In 2020–21, not only did we maintain our hold on high-priority targets, we also stepped up our efforts against some of Australia's most challenging adversaries.

We detected and defeated extremists who are acutely security aware and tech-savvy.

We out-imagined and out-manoeuvred sophisticated foreign adversaries who are effectively unconstrained by law, ethics and resources.

And we did this in the context of a pandemic that had a significant impact on our operating environment. I am proud of the agility and ingenuity that ASIO's officers demonstrated in overcoming the challenges posed by COVID-19.

Threat environment

Australia's threat environment is complex, challenging and changing.

Based on current trends, we anticipate that espionage and foreign interference will supplant terrorism as Australia's principal security concern over the next five years. This is not to downplay the threat of terrorism, which represents an ongoing and evolving challenge. Countering threats to life will always be a priority for ASIO.

Terrorism

Australia's national terrorism threat level remains at **PROBABLE**. This means we have credible intelligence that there are individuals in Australia with the intent and capability to conduct an act of terrorism.

Religiously motivated violent extremists want to kill Australians. Groups such as the Islamic State of Iraq and the Levant (ISIL) continue to urge attacks, 24 convicted terrorism offenders are eligible for release over the next 10 years, and some battle-hardened foreign fighters may yet return to Australia.

At the same time, our investigations into ideologically motivated violent extremists, such as racist and nationalist violent extremists, have grown. During 2020–21, these investigations approached 50 per cent of our onshore priority counter-terrorism caseload.

One of the most concerning aspects of these investigations is the growing number of young people—predominantly young men—who are being radicalised by these ideologies.

It is ASIO's job to identify these threats—to be alert to, and to distinguish the difference between aspiration and capable intent to do harm.

While the possibility of a terrorist attack in Australia—particularly by a lone perpetrator—remains real, we and our law enforcement partners are well positioned to counter this threat.

Espionage and foreign interference

At the same time, espionage and foreign interference attempts by multiple countries remain unacceptably high.

These attempts occur on a daily basis. They are sophisticated and wide-ranging. They are enabled and accelerated by technology. And they take place in every state and territory, targeting all levels of government, as well as industry and academia.

Foreign spies are attempting to obtain classified information about Australia's trade relationships, defence and intelligence capabilities.

They are seeking to develop targeted relationships with current and former politicians, and current and former security clearance holders.

They are monitoring diaspora communities in Australia and, in some cases, threatening to physically harm members of these communities.

Preparation for sabotage

I remain concerned about the potential for Australia's adversaries to pre-position malicious code in critical infrastructure, particularly in areas such as telecommunications and energy. Such cyber enabled activities could be used to damage critical networks in the future.

All these activities represent threats to Australia's way of life. They can undermine Australia's sovereignty, democratic institutions, economy and national security capabilities.

ASIO's response

ASIO has responded to espionage and foreign interference threats with targeted investigations and campaigns that have meaningfully reduced harm. Working with our partners, our activity led to law enforcement outcomes and intelligence-led disruptions. Visas were cancelled and spy networks were dismantled.

These activities have led to a significant reduction in the number of foreign spies and their proxies operating in Australia.

At the same time, we intensified our work with government and industry stakeholders to harden the environment and make it as difficult as possible for foreign spies to operate in Australia.

In late 2020, we launched the Think Before You Link campaign, part of a broader initiative to reduce the risks associated with approaches from foreign intelligence services on social media platforms.

We continue to adapt our counter-terrorism efforts to respond to the changing security environment. Our unique collection capabilities, investigations and analysis continue to identify threats. And our advice has contributed to broader government understanding of the terrorist threat environment within Australia, our near region, and globally. In cooperation with our law enforcement partners, our work has led to arrests and convictions.

In early 2021, we changed the language we use to describe terrorism and violent extremism to better reflect the evolving threat environment. Terms like 'left-wing extremism' and 'right-wing extremism' are no longer fit for purpose when a growing number of extremists do not sit on the left–right spectrum at all.

Instead, we now use religiously motivated violent extremism and ideologically motivated violent extremism as umbrella terms, with more specific terminology available when we refer to particular threats. This new language allows us to more accurately, objectively and flexibly describe the threats Australia faces.

Capability

In May 2021, the Australian Government announced a significant new investment in ASIO's sensitive capabilities. The allocation of $1.25 billion over 10 years will enhance ASIO's ability to "connect the dots" through a human-led, data-driven, technology-enabled approach to threat detection. We will work with the Australian technology sector to deliver this capability.

This investment will also ensure we can maintain our core capabilities and infrastructure.

Late last year, legislation was passed that allows us to be more flexible in our use of less intrusive tracking devices, and to compel suspected spies to attend interviews. We have since used both of these powers; evidence that an evolving threat environment requires evolving capabilities—and that we don't ask for new powers or resources unless we need them.

Transparency

We recognise the importance of using our capabilities and statutory powers responsibly, proportionately, and with propriety. ASIO is committed to acting within the letter and the spirit of the law.

ASIO is subject to stringent oversight, including by the Inspector-General of Intelligence and Security, who has powers akin to a Royal Commission. We welcome this, because it allows us to demonstrate that we operate lawfully and with integrity.

While there will always be a need to protect and safeguard our people and capabilities, I believe in being as transparent as I can with the community about what we do and the nature of the threats facing this country.

This year I appeared regularly at Senate Estimates hearings, and my team engaged regularly with the Parliamentary Joint Committee on Intelligence and Security and the Independent National Security Legislation Monitor.

In March 2021, I delivered my second Annual Threat Assessment. This public address is an important foundation for our efforts to be as open and informative as we can be.

In August 2020, we joined the world of Twitter—another avenue to communicate with the public about who we are and what we do. This was complemented by our recent launch of the ASIO Instagram account.

This annual report is another way in which we demonstrate our commitment to transparency. It sets out our performance against our key priorities of the last 12 months, and shows how we have managed our resources. A copy of this report is available on ASIO's website, as well as at the Australian Government Transparency Portal (transparency.gov.au), which promotes access to annual report content and data across the Australian Public Service.

Mike Burgess
Director-General of Security

2

Overview of ASIO

Overview of ASIO

ASIO protects Australia and Australians from threats to their security.

Our functions are set out in section 17 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

'Security' is defined in section 4 of the ASIO Act as the protection of Australia and its people from:

- espionage;
- sabotage;
- politically motivated violence;
- promotion of communal violence;
- attacks on Australia's defence system; or
- acts of foreign interference;

whether directed from, or committed within, Australia or not; and

- the protection of Australia's territorial and border integrity from serious threats.

ASIO achieves its purpose by obtaining, correlating, evaluating and communicating intelligence relevant to security. Our anticipatory role means we pursue intelligence which enables the detection of adverse security events at their earliest stage.

We protect Australia and Australians by:

- understanding Australia's security environment and identifying security threats;
- hardening the environment against future threats; and
- disrupting threats to reduce harm.

We communicate and advise to inform operational action, government decision-making, policy development and community resilience. We work with other agencies and authorities to achieve outcomes that reduce harm to Australia's national interest.

The Director-General of Security is an independent statutory office holder with specific responsibilities under the ASIO Act to ensure the work of the Organisation is limited to what is necessary to discharge ASIO's functions.

The Director-General is responsible for ensuring ASIO is free from any influences or considerations not relevant to its functions, and to ensure nothing is done that might suggest that ASIO seeks to further or protect the interests of any particular section of the community.

In 2020–21, ASIO pursued its purpose to protect Australia and Australians from threats to their security through five key priorities:

- counter-terrorism;
- counter–espionage and foreign interference;
- border security;
- ASIO's reform program; and
- governance and accountability.

Part 4 of this report summarises our performance in relation to these key activities during 2020–21.

Commitment to legality and propriety

ASIO operates in proportion to the threats Australia faces, within the letter and the spirit of the law, and in line with the standards and expectations of the Australian community. We are subject to a comprehensive oversight and accountability framework which underpins and supports our commitment to legality and propriety.

ASIO's accountable authority

		Period as the accountable authority within the reporting period	
Name	**Position title/ position held**	**Date of commencement**	**Date of cessation**
Mike Burgess	Director-General of Security	15 September 2019	N/A

Mr Mike Burgess, Director-General of Security, was ASIO's accountable authority during the 2020–21 reporting period.

Mr Burgess commenced as Director-General of Security on 15 September 2019.

Ordinary Australians who do extraordinary things

ASIO is an Organisation with a clear mission—to protect Australia and Australians from threats to their security. ASIO's people are its most important asset for achieving its mission—they are ordinary Australians who do extraordinary things. In a complex, challenging and changing security environment, our success is built on the imagination and intelligence of our team.

ASIO's staff routinely do things that seem impossible, but after work they face the same challenges, worries and duties we all have. They are your neighbours, friends and members of your community. They pay mortgages, coach sporting teams, care for loved ones, and volunteer to fight fires or patrol beaches. They are former nurses, teachers, trades specialists, musicians, engineers, athletes and journalists. They are proud Aboriginal and Torres Strait Islander peoples. They are introverted, extroverted and neurodiverse.

Agility and ingenuity are at the core of ASIO's operations. ASIO's staff need to be able to out-think and out-manoeuvre Australia's adversaries. Our people are creative, lateral and critical thinkers. They are problem-solvers and committed team members who want to make a difference.

ASIO requires and desires diversity. We have a diverse and inclusive environment where all staff are valued, respected, included and safe. We want all ASIO officers to bring their whole selves to work, to contribute their unique skills, experiences and perspectives.

In 2020–21 we recruited 116 new staff, and we will continue to build on this over the next 12 months. With diverse roles in analysis, communications, human resources, information technology, intelligence, languages and law, ASIO offers exceptional careers for exceptional people.

Join the mission.

Organisational structure

Mike Burgess
Director-General of Security

Heather Cook
Intelligence Service Delivery

Counter Terrorism	Counter Espionage & Interference	Threat & Security Advice	Digital & Physical Access Capability	HUMINT Capability & Operational Assurance (Snr Rep Nth)	Analysis, Assessment & Advice Capability (Snr Rep Sth)
Counter Terrorism A	Counter Espionage & Interference A	Threat Assessment Centre	Capability & Enablement	HUMINT Capability Development	AAA Capability Development
Counter Terrorism B	Counter Espionage & Interference B	Security Assessments	Computer Operations	Strategic HUMINT & Operational Assurance	Analysis & Discovery
Counter Terrorism C	Counter Espionage & Interference C	Outreach/T4	Close Access Operations		
	Counter Espionage & Interference D		Surveillance		ISD Hub
	Counter Espionage & Interference E				

Figure 1: ASIO's organisational structure at 30 June 2021

Strategic Advisor

Hazel Bennett
Enterprise Service Delivery

Legal Services	Technology & Reform	Enterprise Services	Strategy & Engagement
Legal Advice & Operational Support	Infrastructure	Finance & Procurement	Governance & Strategy
Assessments & Litigation	Business Information Services	Internal Security Services	Government Engagement & Oversight
	Data	People	
	Reform	Learning & Development	
		Facilities Services	
		Investment	

Band 3
Band 2
Band 1

3

Australia's security environment and outlook

Disruptions and attacks 2014–21

Major counter-terrorism disruption *(nationalist and racist violent extremism)*

Major counter-terrorism disruption *(Sunni violent extremism)*

Domestic terrorist attack

Major espionage and foreign interference disruption

Australia's security environment and outlook

Espionage, foreign interference and sabotage

The threat to Australia from espionage and foreign interference is enduring, and sabotage of Australian critical infrastructure is possible. Although legislative change, operational initiatives and the impact of COVID-19 have made the operating environment more difficult for our adversaries, they have adapted their methods without changing their intent.

Espionage

Foreign powers and their proxies, including intelligence services, continue to steal proprietary, sensitive and commercially valuable Australian information. Their efforts harm almost all facets of Australian society at all levels of government in every state and territory, as well as Australia's science and technology sectors, both military and civilian.

Espionage is the theft of Australian information or capabilities for passage to another country, which undermines Australia's national interest or advantages a foreign country.

The COVID-19 pandemic accelerated global digital transformation and uptake of new technologies, altering the way espionage can occur and the corresponding level of harm. Cyber espionage remains the most pervasive approach adopted by our adversaries; it is highly effective and deniable, and can be executed remotely. The Internet of Things and the popularity of social networking sites increase Australia's exposure, while powerful digital tools make our adversaries more effective. Robust cyber security remains critically important in defending Australia from threats to security in the digital age.

The threat is not just from cyber espionage; foreign intelligence services and their proxies are seeking to develop relationships across government, academia and business to steal information. The abundance of personal information online helps foreign intelligence services identify and contact potential targets at all levels, to recruit as human sources. Despite efforts to either remove foreign intelligence officers and their proxies from Australia or hamper their activities, we anticipate the threat from espionage will increase during times of heightened tension.

Foreign interference

Australia remains the target of sophisticated foreign interference by a range of states.

Almost every sector of the community is a potential target for foreign interference. Foreign powers are targeting Australia's parliamentarians, their staff and government officials; the media and opinion-makers; and the business and university sectors. The goal of these foreign powers is to build and leverage community and business relationships to covertly shape decision-making to Australia's detriment—and they are prepared to invest years of effort to do so.

Foreign interference involves clandestine, deceptive or threatening activity conducted on behalf of a foreign power which aims to affect political or governmental processes or is otherwise detrimental to Australia's interests.

Australians, including those from diaspora communities, continue to report that they are being threatened and intimidated by foreign intelligence services to change their behaviour.

Sabotage

Sabotage is damaging or disruptive activity against infrastructure—including electronic systems—to undermine Australia's national security or advantage a foreign power. Acts of sabotage are not limited to irreversible, destructive attacks on physical infrastructure; they can include small-scale, selective and temporary acts of degradation or disruption to networked infrastructure.

The increasingly interconnected nature of Australia's critical infrastructure exposes vulnerabilities which, if targeted, could result in significant consequences for our economy, security and sovereignty. Pre-positioned malicious software—which can be activated at a time of a foreign power's choosing—presents the potential for disruptive or damaging attacks. While we have not observed an act of sabotage in Australia by a foreign power, it is possible—and becomes more likely—when geopolitical tensions increase.

Pre-existing foreign access to Australia's infrastructure, established through foreign investment and/or involvement, and magnified through concentrations of ownership in key sectors, can provide or enhance opportunities for foreign powers and their intelligence services to conduct hostile activities.

Terrorism in Australia

Violent extremists, both religiously and ideologically motivated, continue to pose a threat to the Australian community.

Australia's national terrorism threat level is PROBABLE—credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to conduct a terrorist attack in Australia.

COVID-19 has not substantially diminished the threat of terrorism in Australia. Lockdowns have limited in-person contact, but have probably increased online exposure to violent extremists, both religiously motivated and ideologically motivated, who are seeking to connect, inspire, influence and radicalise.

The proliferation of secure messaging apps means communications can be more anonymous and directly targeted to vulnerable individuals and groups, isolating them from alternative views and hardening their beliefs. Their use also makes detecting attack planning more difficult.

There were two terrorist attacks in 2020–21; and three planned attacks were disrupted over this period. Both terrorist attacks were by lone actors using simple weapons. Future attacks and plans are likely to follow this pattern. Violent extremists across the ideological spectrum are most likely to target easily accessible crowded public places. Any terrorist attack in Australia is more likely to be committed by a lone actor or a small group using simple methods and basic weapons—such as guns, knives or vehicles. This type of threat is difficult to detect, and can emerge with little to no forewarning.

New terminology

In early 2021, ASIO adopted new terminology to describe terrorism and violent extremism to ensure our terminology remains fit for purpose in an evolving threat environment.

The framework uses two umbrella terms for violent extremism—religiously motivated violent extremism, and ideologically motivated violent extremism.

Religiously motivated violent extremism denotes support for violence to oppose or achieve a specific social, political or legal system based on a religious interpretation. Ideologically motivated violent extremism denotes support for violence to achieve political outcomes or in response to specific political or social grievances.

Religiously motivated violent extremists—specifically Sunni violent extremists—remain an enduring threat and continue to be shaped by ISIL and, to a lesser extent, al-Qa'ida. These groups continue to promote attacks against the West by publishing propaganda designed to radicalise, instruct on and inspire terrorist attacks. Australia continues to be specifically mentioned.

Ideologically motivated violent extremists—specifically nationalist and racist violent extremists—remain focused on producing propaganda, radicalising and recruiting others, and preparing for an anticipated societal collapse.

They are security-conscious and adapt their security posture to avoid legal action. Nationalist and racist violent extremists are located in all Australian states and territories. Compared with other forms of violent extremism, this threat is more widely dispersed across the country—including in regional and rural areas. The emergence of nationalist and isolationist narratives globally is normalising aspects of ideologically motivated violent extremist ideology, including nationalist and racist, and specific-issue violent extremism.

Violent extremism and minors

We continue to identify minors who are involved in both religiously motivated and ideologically motivated violent extremism.

Minors have planned and conducted terrorist attacks, occupied leadership positions in violent extremist groups, and radicalised others.

Violent extremist narratives across the spectrum particularly appeal to teenagers, and may resonate with some minors' feelings of alienation, unease about the future and mistrust of adults. Radicalisation can occur quickly and without the knowledge of family or friends. A home-based audience of unprecedented size, pushed online by COVID-19, is likely to have increased exposure to violent extremist propaganda, though minors also continue to be radicalised in-person by peers or older associates.

Communal violence and violent protests

Communal violence in Australia is infrequent, but we have seen isolated incidents involving diaspora communities in Australia reacting to specific events overseas. Communal tensions are generally expressed through public events and demonstrations aimed at drawing the attention of the broader Australian community to specific issues.

There is a limited tradition of violent protest in Australia, and most protests continue to resolve peacefully. While incidental violence has occurred in the past 12 months, it has generally been opportunistic and most likely to occur when events are attended by counter-protesters.

The COVID-19 pandemic has been used by issue-motivated groups to promote their individual views. These groups are seeking to exploit social and economic dislocation, and their ideology has been spreading more quickly and widely as Australians spend more time online.

Terrorism—the international security environment

South-East Asia

Despite COVID-19 restrictions largely constraining the movement of violent extremists, those in South-East Asia collaborate and consume ISIL propaganda online, and also plan and conduct simple—often opportunistic—attacks, primarily directed against local security forces and sectarian targets. Under ISIL's influence, religiously motivated violent extremists are adapting their methods, with suicide bombings becoming more common in the southern Philippines and attacks by females and families occurring across the region more broadly.

Al-Qa'ida-aligned groups also continue to recruit, train and prepare for possible future violence. Cross-border connections, both in the region and into international conflict zones, increase the risk that skills, attack methods and ideology will be transferred between religiously motivated violent extremist groups across the world.

The scheduled release of terrorist detainees in South-East Asia, many of whom probably maintain violent extremist ideologies, will be detrimental to the security environment in the region.

South and Central Asia

Attacks by religiously motivated violent extremists continued throughout 2020–21, particularly in the less-governed areas of Afghanistan and Pakistan. Attacks on government interests, security forces and minorities will continue, particularly in Afghanistan where the security environment has further deteriorated. High-profile attacks by terrorist groups, including Islamic State—Khorasan Province (IS-KP), will persist.

Elsewhere in the region, violent extremist narratives—typically religiously motivated, but including those that are ideologically motivated—are still radicalising individuals and groups which primarily conduct basic attacks. Although a small-scale attack, the May 2021 improvised explosive device attack in the Maldives indicates that violent extremists operating there have an interest in conducting more complex attacks.

The impact of COVID-19 on South Asia increased in mid-2021, but its effect on the terrorist threat remained limited. While decreased tourism reduces the likelihood of Westerners being attacked, the anti-Western intent of some violent extremists is unchanged.

Middle East

ISIL's post-caliphate insurgency persists in Syria and Iraq. Although ISIL has not reclaimed territory, and continues to lose senior leaders and fighters, it maintains a high attack tempo in these countries, and continues to inspire and direct attacks. Low-capability Sunni violent extremist attacks will persist across the Middle East, mostly posing the threat of incidental harm to Australian interests.

Al-Qa'ida-affiliated or al-Qa'ida-linked groups continue to exploit civil unrest and ungoverned spaces in the Middle East—particularly north-west Syria and Yemen—and remain intent on attacking Western interests. Al-Qa'ida will prioritise its longevity and adapt to work with local sympathisers. Large-scale attacks are unlikely, but basic attacks by individuals and groups—driven by local issues and objectives—will persist.

Separate to ISIL and al-Qa'ida, nationalist and revolutionary violent extremists continue to pose a threat. In May 2021, an 11-day conflict followed rising tensions in Israel and the Palestinian Territories. The conditions for cyclical violence remain, despite a fragile ceasefire. In Iraq and Turkey, Kurdish militants continue to clash with Turkish authorities over a separate Kurdish state and identity.

Iran-backed Shia militia groups in Iraq will almost certainly continue to target United States (US) and Coalition interests, in an attempt to effect a US Coalition withdrawal from Iraq. Tensions between the US and Iran will continue to destabilise the region.

Europe and North America

Terrorist attacks and disruptions in Europe—including in Austria, France and Germany—highlight the persistent threat posed by religiously motivated violent extremist attacks. Such attacks are most likely to be inspired by Sunni violent extremism and use basic weapons—such as knives, vehicles, firearms and/or explosives—to target crowded places or police and uniformed personnel. The release of terrorist prisoners across Europe is likely to exacerbate the terrorist threat.

Individuals or small cells motivated by nationalist and racist or specific-issue violent extremism are more likely to pursue violence than established groups. These types of violent extremists primarily pose a threat to Jewish, Muslim or other minorities, as well as ideological opponents.

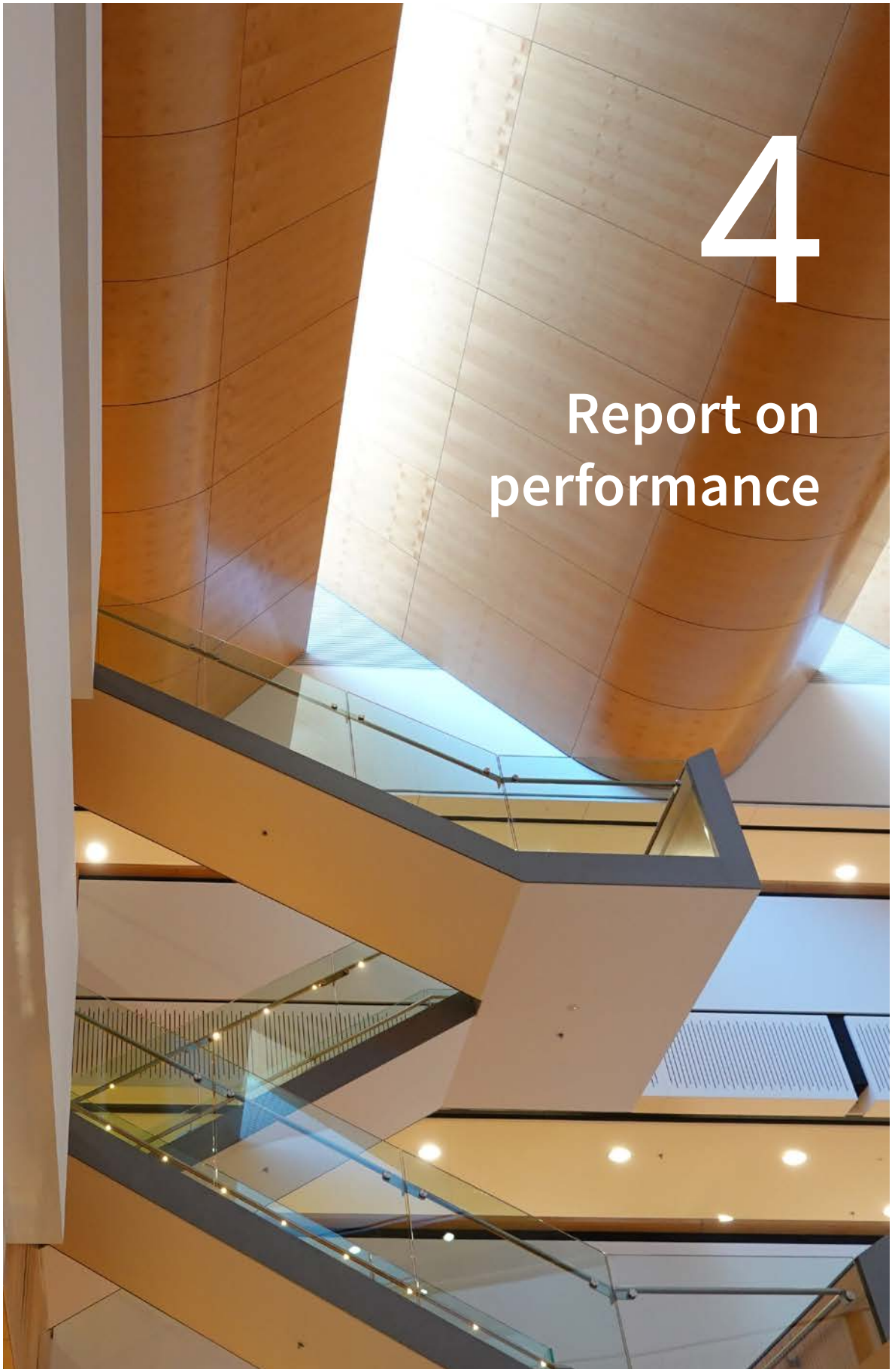
Africa

In Africa, established -aligned and ISIL-aligned groups continued their attacks aimed at destabilising regional governments. Emerging ISIL affiliates have gained strength, including in northern Mozambique—demonstrated by their concerted March and April 2021 attacks on foreign mining operations in the northern province of Cabo Delgado which killed several foreigners. And from Mali, terrorist groups have expanded their areas of operation into neighbouring Burkina Faso, Niger and some coastal states. Most terrorist groups in Africa will target Westerners, including Australians, if they have the opportunity.

Border security

The demand for irregular maritime ventures to Australia remains suppressed. COVID-19 global travel restrictions and lockdown measures offshore have created a particularly difficult operating environment for people smugglers. Despite this, attempts at irregular maritime migration to Australia and our region occurred throughout the period at low levels.

While deteriorating economic, health or security conditions in the source countries of potential irregular immigrants have the potential to drive individuals to take desperate measures to escape such conditions in the future—possibly through irregular migration to Australia—there is no evidence that this has occurred in the last 12 months. Potential irregular immigrants remain aware that there is a low prospect of permanent resettlement in Australia, which reduces demand for irregular maritime ventures to Australia.



4

Report on performance

Annual performance statement 2020–21

Introductory statement

I, as Director-General of Security and the accountable authority of ASIO, present the 2020–21 annual performance statements for ASIO, as required under subsection 39(1)(a) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act). In my opinion, these statements accurately present the performance of ASIO in achieving its purpose and comply with subsection 39(2) of the PGPA Act.

Mike Burgess
Director-General of Security

Reporting framework

ASIO operates under the Australian Government's outcomes and programs framework. Outcomes are the intended results, impacts or consequences of a purpose or activity by the government as defined in the portfolio budget statements for Commonwealth entities.

Performance reporting requirements are part of the Commonwealth Performance Framework established by the *Public Governance Performance and Accountability Act 2013*.

It is anticipated this performance statement will be read with broader information provided in the *ASIO Corporate Plan 2020–24* and the Home Affairs Portfolio Budget Statements (PBS) to provide a broad picture of ASIO's planned and actual performance.

The alignment between ASIO's purpose, as set out in the *ASIO Corporate Plan 2020–24*, and the Outcome and Program in the ASIO PBS is shown below.

ASIO Portfolio Budget Statements	Portfolio Outcome 1
	To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to government
	Program 1.1 Security Intelligence
	ASIO operates a single program—Security Intelligence—focused on delivering Outcome 1.
ASIO Corporate Plan 2020–24	ASIO's Purpose
	To protect Australia and Australians from threats to their security
	Key performance measures 1–9
Annual Performance Statements 2020–21	Report against key performance measures

ASIO's purpose

ASIO's purpose is to protect Australia and Australians from threats to their security, as defined in the *ASIO Corporate Plan 2020–24*.

In 2020–21, ASIO achieved this purpose through delivering outcomes against each of the Organisation's key priorities below.

Counter-terrorism

ASIO protects Australians from politically motivated and communal violence. We do this by collecting intelligence here and overseas; analysing and investigating terrorism threats; and providing advice to, and working with, partners to strengthen public safety and intervening to disrupt attacks.

Counter–espionage and foreign interference

ASIO protects Australia from efforts by hostile foreign intelligence services to undermine Australia's democratic systems and institutions. We do this by collecting intelligence to detect and deter espionage and foreign interference activities targeting Australian interests here and overseas, investigating threats and advising government and industry partners as we work with them to foster institutional and community resilience.

Border security

ASIO supports whole-of-government efforts to protect Australia's border integrity through intelligence collection and investigations into people smuggling activities. We provide unique analysis of, and security advice on, complex visa applications and other movements of goods and people, to advance the efforts of our partners in maintaining Australia's economic and national security interests.

Reform program

ASIO is committed to accelerating the delivery of our mission through improvements to our technology. ASIO's reform program will modernise our data analytics and increase the speed and scale of our discovery and investigative work; and deliver reforms across the Organisation to improve effectiveness in our decision-making, resolve threats quickly and drive down risk.

Governance and accountability

High levels of public trust are critical to ASIO's operations and the effective and efficient delivery of our purpose. ASIO achieves this through strict compliance with the law, stringent application of policies and procedures, and our active cooperation with external oversight. ASIO is committed to the continual improvement of our enterprise management and governance practices to assure Australians that we pursue our work with integrity and accountability.

Performance measures

This annual performance statement provides an assessment of ASIO's achievement of the performance measures set out in the *ASIO Corporate Plan 2020–24*.

The measures relating to counter-terrorism, counter–espionage and foreign interference, and border security (measures 1–6) focus on the level of impact of ASIO advice (operational and/or policy). When assessing impact, we considered whether:

- ASIO advice provided context;
- ASIO advice was relevant and practical; and
- ASIO advice influenced stakeholder decision-making.

For the purposes of this report, 'advice' encompasses all forms of communication to the Australian Government, government agencies, and industry and community sector stakeholders that conveys ASIO's expertise, intelligence, assessments, priorities and recommendations on security matters.

The following definitions were shared with key stakeholders when determining what level of impact our advice (policy and/or operational) has had on their decision-making.

LOW	MEDIUM	HIGH
Our advice provided little or no context, and did not influence your decision-making.	Our advice provided context; was relevant and practical; and, influenced your decision-making.	Our advice was timely and relevant; practical, focused and provided or enabled exercisable options; and directly informed and shaped your decision-making.

The remaining key priorities (measures 7–8—ASIO reform program, and measure 9—governance and accountability) focused on establishing a baseline for internal programs and utilised maturity assessments against industry standards and internal staff satisfaction surveys.

Performance methodology

Performance against our priorities has been measured through a combination of quantitative and qualitative methods, including defined targets, case studies, external surveys, stakeholder feedback, and identified milestones.

In 2020, for the first time, we introduced specific performance measures designed around percentage-based impact targets. Redesigning our measures in this way was a deliberate decision to measure outcomes against our key priorities rather than outputs. Measuring outcomes in this way is important to ensure we are focusing our efforts and delivering meaningful change for stakeholders.

The ASIO stakeholder survey collected quantitative and qualitative data on ASIO's performance from 64 stakeholders across government, tertiary and private sectors.

Given this was the first time ASIO has used percentage-based impact targets, we will continue to refine these measures—including the methodology, stakeholders, and targets—over time, in order to more accurately measure our impact across the spectrum of our work.

Qualitative and quantitative methodologies

Key performance measures	Defined targets	Case studies	External surveys	Stakeholder feedback	Identified milestones
1	✓	✓	✓	✓	
2	✓	✓	✓	✓	
3	✓	✓	✓	✓	
4	✓	✓	✓	✓	
5	✓	✓	✓	✓	
6	✓	✓	✓	✓	
7	✓			✓	✓
8	✓			✓	
9	✓				✓

Summary of results

ASIO has achieved significant outcomes against the ambitious targets it set for itself in 2020–21. ASIO met seven of its nine performance measures, and partially achieved the remaining two.

In the context of a complex, challenging and changing threat environment, ASIO continued to protect Australia and Australians against terrorism. Our work enabled disruptions and supported law enforcement arrests and convictions. Our achievements represent a continuation of ASIO's high performance in contributing to policy advice and counter-terrorism operational activity over the last 20 years. These efforts were supported by mature frameworks spanning policy, intelligence and law enforcement. ASIO is well positioned to address future challenges in the terrorism environment, such as the increasing prevalence of ideologically motivated violent extremism and growing numbers of radicalised minors.

In parallel, ASIO activities have had a significant impact on the threat of espionage and foreign interference. In 2019–20, we assessed that this threat was unprecedented. Over the last 12 months, and in the context of maturing legislative frameworks, ASIO has concertedly worked to address this threat by hardening the environment and disrupting high-harm espionage and foreign interference activity. Our cooperation with law enforcement colleagues through the ASIO-led Counter Foreign Interference Taskforce has supported this effort.

While the threat continues at an unacceptably high level, and is likely to supplant the threat of terrorism in coming years, it is no longer accurate to describe the threat as 'unprecedented'. ASIO remains well positioned to continue to protect Australia and Australians from foreign interference and espionage.

ASIO has also continued to support whole-of-government efforts to protect the integrity of Australia's border, commensurate with the changing border environment resulting from the COVID-19 pandemic.

Supporting these efforts is the work we have undertaken to reform our capabilities, and our improvement of governance and accountability practices. Delivery of these priorities continues to enable the acceleration of our mission delivery against our key priorities.

Performance measures

Counter-terrorism

ASIO protects Australians from politically motivated and communal violence. We do this by collecting intelligence here and overseas; analysing and investigating terrorism threats; and providing advice to, and working with, partners to strengthen public safety and intervening to disrupt attacks.

Counter-terrorism

Result—impact of ASIO's counter-terrorism policy development advice

1. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a HIGH impact on their decision-making in relation to policy development and responses to terrorism.			
Target	2020–21	80%; HIGH	Outcome	PARTIALLY ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 7) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

The stakeholder survey results in relation to our 'Counter-terrorism—impact of policy development advice' measure were positive overall, particularly in relation to ASIO's partnership efforts. One hundred per cent of respondents indicated ASIO had achieved a **MEDIUM** or higher impact with 56 per cent of respondents reporting ASIO advice had achieved a **HIGH** impact. This outcome is below the ambitious target we set ourselves in the *ASIO Corporate Plan 2020–24*. Our counter-terrorism policy advice was delivered in the context of mature policy frameworks. In combination with the threat environment, these mature frameworks have resulted in a reduced demand for advice to inform policy settings.

The survey recorded a significant quantity of positive feedback, which rated ASIO as providing advice that was useful in shaping or informing counter-terrorism policy development. The survey results also demonstrated that ASIO advice has greatly assisted a number of intelligence agencies prioritising within their counter-terrorism programs.

ASIO's advice and assessments in relation to dual-citizen foreign fighters was commented on positively. One state government department advised that it relied on ASIO advice to inform updates to relevant state legislation and to inform the state's approach to countering violent extremism. Other feedback noted that tactical details provided by ASIO directly supported strategic judgements made by other National Intelligence Community agencies.

Additional feedback captured from stakeholders through engagements throughout the year was overwhelmingly positive.

ASIO continued to engage closely with our counter-terrorism partners—and provide assessments and advice drawn from our unique collection, investigation, and analysis capabilities, with favourable outcomes.

Examples demonstrating ASIO's impact on stakeholder policy development include the following.

Our advice provided context

- In September 2020 ASIO provided advice, as part of a joint initiative with a partner agency, to a state government department on the impact of the COVID-19 pandemic on social cohesion in Australia (and in the online environment). The advice supported the state's countering violent extremism program efforts.
- In April 2021, ASIO published advice on the Australian elements of one of the groups involved in the Capitol violence in Washington, US. Our advice was informed by our investigations into, and analysis of, issue-motivated violent extremists; and provided context for domestic partner agency responses to this and other similar groups.
- ASIO received positive feedback from the private sector on assistance it provided in the development of a Standards Australia handbook on physical protective security controls of buildings. This work will help to shape building design in Australia to protect against terrorist threats, and build the baseline of protective security knowledge across the sector.

Our advice was relevant and practical

- In August 2020, ASIO advice on the impact of COVID-19 on global and Australia-based counter-terrorism directly informed Department of Home Affairs policy and program considerations for countering violent extremism, social cohesion and community engagement.
- In August 2020, ASIO provided the Minister for Home Affairs with advice about an Australian citizen and their affiliation with Islamic State in Libya, contributing to the first citizenship cessation case for activities conducted outside the Syria–Iraq conflict zone.

Our advice influenced decision-making

- In December 2020, ASIO provided Home Affairs with a brief on listed terrorist organisations Islamic Movement of Uzbekistan and Lashkar-e-Jhangvi, which highlighted the significant reduction of attack planning attributed to both groups. ASIO advice informed the Home Affairs proposal to not relist the Islamic Movement of Uzbekistan and Lashkar-e-Jhangvi under the Criminal Code.
- In February 2021, ASIO provided a brief to Home Affairs on United Kingdom–based nationalist and racist violent extremist group Sonnenkrieg Division. This brief supported the Home Affairs statement of reasons for listing the group as a terrorist organisation under the Criminal Code. ASIO advice directly contributed to the decision that Sonnenkrieg Division met the legal threshold for listing.

- Some nationalist and racist violent extremists seek to join the Australian Defence Force to obtain training and capability. ASIO and Defence have worked closely to ensure ASIO security assessment processes can be applied proactively to these individuals. As of May 2021, a new framework was agreed to, leading to ASIO receiving related referrals from Defence.

During the reporting period, our advice and intelligence informed whole-of-government efforts to mitigate the terrorist threat to Australians and Australian interests, including the following:

127 187
access security assessments

114 832

to AusCheck, including for individuals seeking Aviation Security Identification Cards (ASICs) and Maritime Security Identification Cards (MSICs)

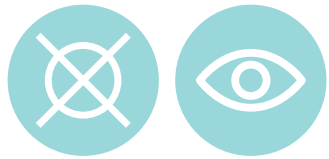
12 355

individuals seeking access to security-sensitive chemicals, biological agents or nuclear sites

618

counter-terrorism products

69



products that span both counter-terrorism and counter–espionage and foreign interference

Result—impact of ASIO's counter-terrorism operational activities advice

2. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a HIGH impact on their decision-making in informing counter-terrorism operational activities, managing security risks and disrupting activities that threatened Australia's security.			
Target	2020–21	80%; HIGH	Outcome	PARTIALLY ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 7) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

The stakeholder survey resulted in largely positive responses about the impact of our counter-terrorism operational activities advice. A total of 93 per cent of respondents indicated ASIO had achieved a **MEDIUM** or higher impact with 58 per cent of respondents reporting ASIO advice had achieved **HIGH** impact. This outcome is below the ambitious target we set out in the *ASIO Corporate Plan 2020–24*. Our results reflect mature and effective counter-terrorism frameworks, particularly the well-established relationships and arrangements that facilitate joint intelligence and law enforcement activities.

Stakeholders provided a significant number of positive comments on ASIO's support to operational activity. The early advice we provided was valuable in informing decision-making and operations. ASIO is seen as providing timely advice and playing an important role in bringing agencies together to further whole-of-government objectives.

Additional feedback captured throughout the year further demonstrated positive outcomes from ASIO's support to operational activities. Key themes included the value of ASIO's advice in informing decision-making and operations relating to foreign fighters; assistance with prioritisation, passport, citizenship and consular matters; and proactive support to federal and state-based police forces.

Examples demonstrating ASIO's impact on operational activities include the following.

Our advice provided context

- ASIO reporting throughout the 2020–21 year has continued to support Home Affairs portfolio partners and other stakeholders in managing the return of Australian foreign fighters and Australians of counter-terrorism interest, to maximise the control and readiness of the receiving jurisdiction.

Our advice was relevant and practical

- In September 2020, ASIO deepened its collaboration with industry partners on counter-terrorism discovery by providing declassified versions of our reporting on terrorism indicators. This material provided practical advice on the indicators ASIO uses to identify new threats to security. This collaboration has informed and shaped partners' efforts to detect and report on individuals who have purchased improvised explosive device precursors and other extremist material.
- In December 2020, an individual was found guilty in relation to a foreign incursions offence. This concluded an investigation which was initiated by ASIO operational activity based on foreign partner lead reporting. The ASIO investigation into this individual was subsequently handed over to a state-based Joint Counter Terrorism Team, leading to the individual's arrest. This example demonstrates the success that can be generated from ASIO's operational advice and the close working relationships we have established with state-based Joint Counter Terrorism Teams.
- As part of ongoing collaboration with police partners, ASIO provided a coordinated briefing program on nationalist and racist violent extremism, lone actor indicators, and symbols and key texts that officers may encounter in their work.

  After one of these sessions, law enforcement officers attending a crime scene identified a large volume of literature and firearms related to nationalist and racist violent extremism, resulting in a referral for further investigation.

Our advice influenced decision-making

- Throughout 2020–21, ASIO continued to provide support to Joint Counter Terrorism Teams around Australia—including advice and assessments which assisted with operational activities, and the prosecution, sentencing, and release of various individuals for terrorism and related offences.
- In April 2021 ASIO provided actionable intelligence to law enforcement partners about an individual expressing intent to undertake an act of politically motivated violence. ASIO advice directly informed Joint Counter Terrorism Team operational activity, resulting in criminal charges and the arrest of the individual, therefore mitigating any imminent threat he may have posed to the community.
- In June 2021 ASIO collaborated with National Intelligence Community partners on a series of briefings to Joint Counter Terrorism Teams. Our religiously motivated violent extremism and ideologically motivated violent extremism teams provided context and case studies to assist Joint Counter Terrorism Team members in their investigations.

- In November 2020 an individual was sentenced to 16 years imprisonment with a non-parole period of 12 years after being found guilty at retrial in April 2020 for acts done in preparation for a terrorist act. The sentencing concluded a Joint Counter Terrorism Team investigation that commenced in Sydney in 2016 with the arrest of two 16-year-olds detected carrying knives in a public place, who have now both been convicted and sentenced for a terrorism offence. Both received the same sentence and will be eligible to apply for parole in 2028, and for release in 2032.
- In November 2020 Philip Galea was sentenced to 12 years imprisonment with a nine-year non-parole period on one count of collecting or making documents likely to facilitate a terrorist act contrary to section 101.5 of the Criminal Code, and one count of acts done in preparation for, or planning, terrorist acts, contrary to section 101.6 of the Criminal Code. The charges related to a 2016 plot to attack a range of potential targets including Melbourne Trades Hall, the Anarchist Book Shop, and the Resistance Centre—which is the headquarters of the Socialist Alliance. Galea is the first Australian with an ideologically motivated violent extremist ideology—specifically, nationalist and racist—convicted under Australia's counter-terrorism laws. Galea was arrested on 6 August 2016, and convicted on 5 December 2019.

Case study—counter-terrorism disruptions

Most counter-terrorism disruptions originate from ASIO intelligence investigations. In accordance with our statutory functions, we discover and pursue threat leads which then transition to police-led criminal investigations. ASIO's support to partners includes providing assessments, advice and operational coordination.

There have been three major counter-terrorism disruptions in the past year. ASIO worked with partners to achieve these outcomes.

In November 2020 a Queensland man was arrested and charged with preparing or planning for a terrorist act. In February 2021 a man who was on remand was arrested for allegedly planning a series of violent extremist acts. In March 2021 two Victorian men were arrested and charged with a range of terrorism-related offences, including attempting to engage in a terrorist act. All three matters remain before the courts.

In addition, in December 2020 the New South Wales (NSW) Joint Counter Terrorism Team arrested and charged a man based in NSW with terrorism-related offences. It will be alleged in court the man used social media forums to encourage other people to commit violent acts in support of a nationalist and racist violent extremist ideology. The man was charged with Commonwealth terrorism offences, including advocating terrorism.

Counter–espionage and foreign interference

ASIO protects Australia from efforts by hostile foreign intelligence services to undermine Australia's democratic systems and institutions. We do this by collecting intelligence to detect and deter espionage and foreign interference activities targeting Australian interests here and overseas, investigating threats and advising government and industry partners as we work with them to foster institutional and community resilience.

Counter–espionage and foreign interference

Result—impact of ASIO's counter–espionage and foreign interference policy development advice

3. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our counter–espionage and foreign interference advice had a MEDIUM impact on their decision-making in relation to espionage and foreign interference–related policy development and responses to this threat.			
Target	2020–21	70%; MEDIUM	Outcome	ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 8) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

The stakeholder survey results indicate ASIO exceeded the target of 70 per cent of respondents providing a rating of **MEDIUM** level of impact on counter–espionage and foreign interference policy development, with 100 per cent of respondents reporting ASIO advice had a **MEDIUM** or higher level of impact on their decision-making.

ASIO's increasingly prominent counter-espionage and counter–foreign interference efforts were highly regarded by our stakeholders. In the context of maturing espionage and foreign interference legislative and policy frameworks, ASIO's advice is regarded as being very influential; and ASIO is seen as an essential partner.

Survey respondents also commented that ASIO's advice had been highly valuable in determining positions, informing priorities and assisting decision-making. Respondents noted an increased level of advice, contact and collaboration had occurred over the reporting period.

Additional reporting on our counter–espionage and foreign interference policy–related workflows collected from stakeholders throughout the year supports the assessment that our advice is having, at a minimum, a **MEDIUM** level of impact on stakeholder decision-making.

The 2020–21 reporting period saw a continued upward trajectory in government and private sector demand for ASIO counter–espionage and foreign interference advice and solutions, with ASIO working closely with stakeholders to promote and facilitate improved security practices and advocate policy settings that will provide for Australia's security into the future.

Examples demonstrating ASIO's impact on stakeholder policy development include the following.

Our advice provided context

ASIO contributed to increasing resilience by providing contextual protective security advice to government and private sector stakeholders.

- We published a range of intelligence and security products during the reporting period to support the development of policy to counter espionage and foreign interference.

ASIO provided protective security and defensive counter–espionage and foreign interference advice which improved consistency in policy messaging across the Australian Government, including advice to Commonwealth parliamentarians regarding foreign interference activities and the threat from malicious insiders.

- Advice was provided to ministers and their offices on the threat of foreign intelligence services targeting the Australian Government, including delegations travelling overseas, and measures to mitigate this threat.
- Advice was provided to the Australian Government on the threat of foreign interference in our political system and the targeting of Australians for foreign intelligence collection purposes.
- The Attorney-General's Department advised that ASIO's feedback on insider threat policy guidance was useful and assisted consistency in policy messaging across the Australian Government.

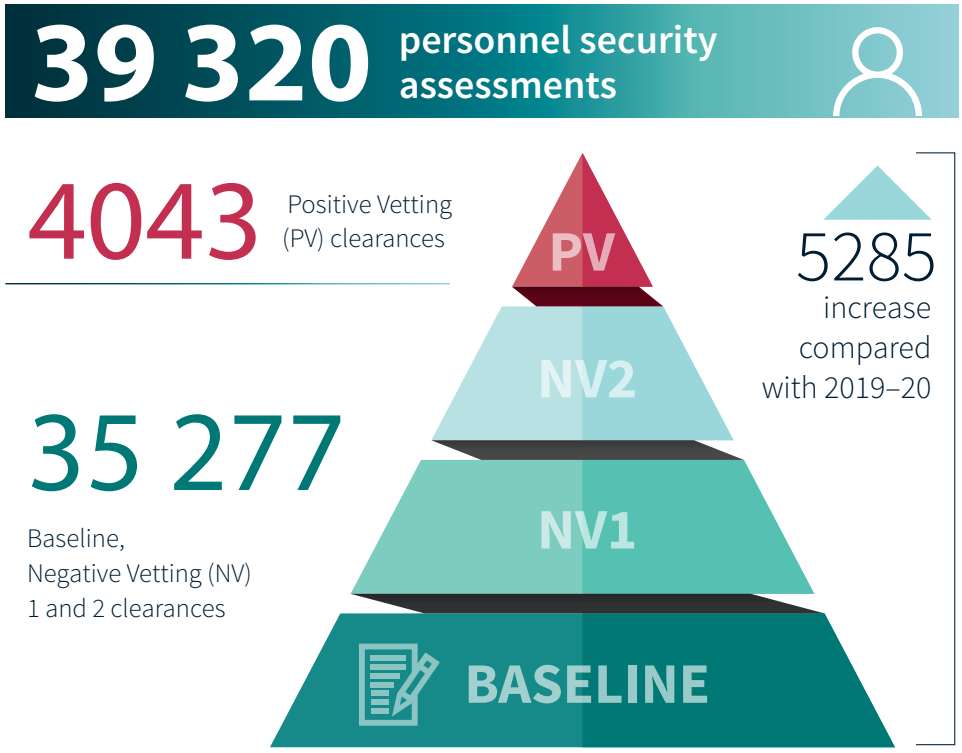
Our advice was relevant and practical

ASIO provided relevant and practical advice to government departments, which led to positive security decisions and beneficial security outcomes.

- We provided advice to the Department of Foreign Affairs and Trade (DFAT) on foreign intelligence services use of academic cover organisations to target Australian interests. This advice informed DFAT officers in their routine engagement with foreign academics.
- We provided advice on security culture and contact reporting processes to a range of government departments.
- Awareness of foreign interference threats in Australia's political institutions and processes was increased through advice from the Director-General to senior decision-makers across the Australian Government and state and territory governments, such as departments of Premier and Cabinet or equivalent.

Our personnel security assessments continued to play a pivotal role in assisting the Australian Government to manage threats to Australia's national security associated with access to privileged government information, places, activities and capabilities.

- In 2020–21, we completed 39 320 personnel security assessments, comprising 35 277 assessments for Baseline, Negative Vetting (NV) 1 and 2 clearances and 4043 Positive Vetting (PV) clearances. This is an increase of 5285 completed assessments compared with the previous year.
- The increased number of cases completed in 2020–21 continued a trend of growth in overall personnel security assessment workload and indicates the increasing demand for personnel security assessments.
- More than 150 personal security briefings were completed. These are used to provide security advice to the subject of an ASIO personnel security assessment to allow them to better understand specific security risks relevant to them and to detail actions to limit and manage those risks.
- We also completed a number of adverse and qualified personnel security assessments, containing information and recommendations about an individual's suitability to be granted or continue to hold a clearance.



Our advice influenced decision-making

Throughout the reporting period we continued to deepen our relationships across government and the private sector to discover, disrupt and deter threats to Australia and Australians and significantly reduce harm. Examples of the impact of ASIO advice on informing partner policy initiatives include the following.

- ASIO advice influenced the internal processes of Australian universities, and generated positive feedback from the universities' senior executives.
- ASIO received positive feedback on our advice from Outreach subscribers, including that our advice prompted discussions with internal security areas within industry and government.
- Supporting whole-of-government diplomacy efforts in the Indo-Pacific, ASIO assessment processes for proposed inward foreign investment was briefed to a foreign government resulting in a request for further advice on critical infrastructure protection.

In 2020–21 ASIO continued to provide key stakeholders across government—including the Critical Infrastructure Centre within Home Affairs, the Department of Defence, Treasury, and the Foreign Investment Review Board—with advice on the threat posed by foreign ownership and control of critical infrastructure.

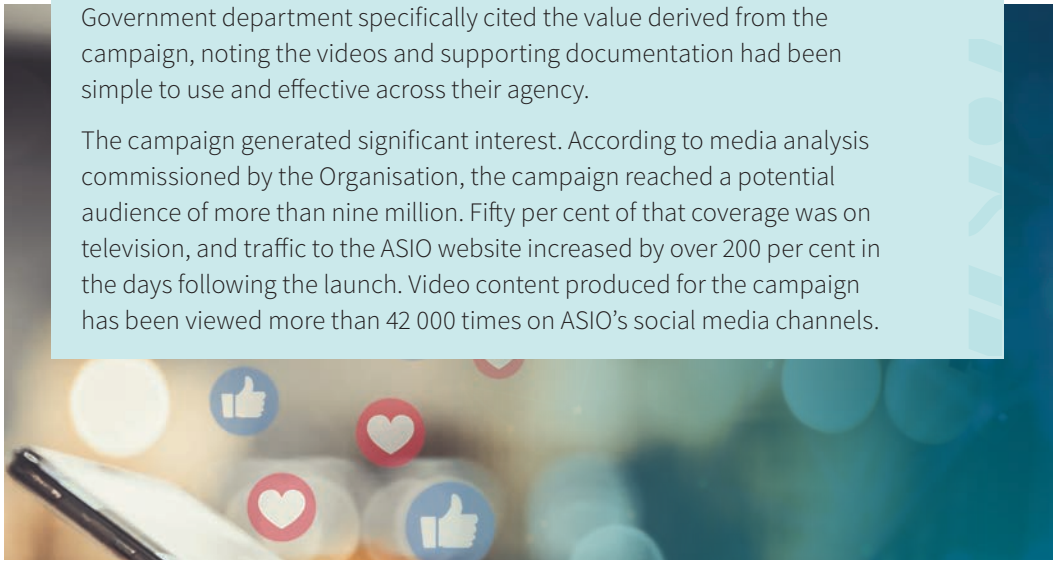
- For the financial year 2020–21, ASIO responded to 457 investment applications received from Treasury in support of the Foreign Investment Review Board's consideration of foreign investment proposals. Our assessments of these applications concern the potential for foreign powers to undertake espionage, foreign interference or sabotage as a result of overseas investment in critical infrastructure and other sensitive sectors of the economy.

Case study—Think Before You Link campaign

ASIO delivered its first public awareness campaign, Think Before You Link, to government and industry customers in November 2020. The campaign raised awareness of the threat posed by malicious social media profiles and provided guidance on how to minimise the risk of being targeted through professional networks and other online platforms.

Government and industry customers have deployed the campaign materials internally to communicate ASIO's messaging directly to staff worldwide. Several state and territory governments and industry customers said that the campaign informed their decision-making. One prominent Australian Government department specifically cited the value derived from the campaign, noting the videos and supporting documentation had been simple to use and effective across their agency.

The campaign generated significant interest. According to media analysis commissioned by the Organisation, the campaign reached a potential audience of more than nine million. Fifty per cent of that coverage was on television, and traffic to the ASIO website increased by over 200 per cent in the days following the launch. Video content produced for the campaign has been viewed more than 42 000 times on ASIO's social media channels.



Result—impact of ASIO's counter–espionage and foreign interference operational activities advice

4. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our counter–espionage and foreign interference advice had a MEDIUM impact on their decision-making in informing counter–espionage and foreign interference operational activities, managing security risks and disrupting activities that threatened Australia's security.			
Target	2020–21	70%; MEDIUM	Outcome	ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 8) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

Results from the stakeholder survey show that 89 per cent of stakeholders rated ASIO's performance as having a **MEDIUM** or higher impact on their decision-making.

Within maturing coordination frameworks, ASIO's advice was useful in shaping or informing counter–espionage and foreign interference operational activities. Our advice was well received, had become more timely and expansive, and had been influential in informing operational decisions.

Additional feedback provided by stakeholders throughout the year supports the assessment that our advice had a **MEDIUM** level of impact on stakeholder decision-making in relation to their operational activities.

Examples demonstrating ASIO's impact to operational activities include the following.

Our advice provided context

During 2020–21 ASIO continued our focus on supporting the development of counter–espionage and foreign interference capability across government and the private sector. Our ability to provide advice is derived from the insights we gain from our investigative work, and this advice had a direct impact on the operational decision-making of our key stakeholders providing context through which positive security outcomes were achieved.

- The Australian Government Security Vetting Agency provided favourable feedback on collaboration and improvements to information exchange processes.
- ASIO provided intelligence advice to a state law enforcement partner about a target assessed to be engaged in foreign interference activities. This advice provided additional context to the partner's separate criminal investigation, which was not related to espionage and foreign interference.

The law enforcement partner's subsequent overt activities were assessed to have disrupted the target's foreign interference activities.

- ASIO contributed to identifying and responding to an ongoing cyber espionage campaign against Australian Government targets and service providers, thereby mitigating significant harm and informing the Australian Government's policy response.

Our advice was relevant and practical

- ASIO provided intelligence to the Australian Federal Police (AFP), via the Counter Foreign Interference Taskforce, about an Australian citizen whom we assessed to be in a clandestine relationship with a foreign intelligence service. ASIO's intelligence assisted the AFP's ongoing investigation into this target, and informed their planning and execution of warranted activities aimed at collecting evidence on potential espionage and foreign interference offences. We assess that the AFP's overt actions have disrupted this individual's foreign interference activities.
- In February 2021, ASIO provided a briefing to a Universities Australia workshop to increase understanding of the security risks associated with foreign involvement in sensitive research. The workshop was attended by 100 senior university representatives, and feedback on ASIO's support was extremely positive.

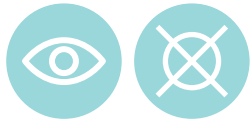
Our advice influenced decision-making

- ASIO provided advice to the Department of Home Affairs on the subjects of our foreign interference investigations, which informed Home Affairs decisions to cancel Australian visas, effectively reducing the harm being perpetrated by the visa holders.
- In 2020–21, the Counter Foreign Interference Taskforce delivered programs to build awareness of foreign interference matters among partners. These programs are a critical component of efforts to improve interoperability and collaboration between law enforcement and intelligence agencies.

During the reporting period, ASIO provided the following:

214

Counter–espionage and foreign interference products



69

Products that span both counter–espionage and foreign interference and counter-terrorism

Case study—nest of spies

In 2020 an ASIO investigation focused on disrupting a 'nest of spies' which was operating in Australia.

The activities undertaken by the foreign service had the potential to cause significant harm to Australia's interests and those who reside in our communities. Notably, the foreign intelligence officers successfully cultivated and recruited an Australian Government security clearance holder with access to sensitive information. They sought to obtain classified information about Australia's trade relationships and gain access to technology not otherwise available to them.

The foreign intelligence agency developed targeted relationships with current and former politicians, Australians with access to privileged and classified information, and community leaders who favoured the foreign agency's agenda and monitored their country's diaspora community.

Through our disruption activities—cancelling the government employee's security clearance, confronting the foreign spies and removing them from Australia—we are confident we have degraded this foreign service's ability to conduct adverse intelligence activities in Australia. We continue to monitor for any evidence the service is attempting to rebuild capacity to undertake undeclared intelligence activity in Australia.

Border security

ASIO supports whole-of-government efforts to protect Australia's border integrity through intelligence collection and investigations into people smuggling activities. We provide unique analysis of, and security advice on, complex visa applications and other movements of goods and people, to advance the efforts of our partners in maintaining Australia's economic and national security interests.

Border security

Result—impact of ASIO border-related policy development advice

5. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our advice on countering serious threats to Australia's border integrity, security-sensitive areas or substances had a **MEDIUM** impact on their decision-making in relation to policy development and responses to serious threats to Australia's border integrity, security-sensitive areas or substances.			
Target	2020–21	70%; MEDIUM	Outcome	ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 9) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

Stakeholder survey results show that 100 per cent of stakeholders surveyed rated ASIO's performance as having a **MEDIUM** or higher impact. ASIO's advice was useful in shaping or informing border security policy development, and was of good quality.

Additional reporting gathered internally on our border policy–related workflows also demonstrated that our advice had a **MEDIUM** level of impact on stakeholder decision-making. ASIO continued to provide actionable policy-related advice to key Australian Government border security partners, including DFAT and Home Affairs portfolio agencies such as the AFP and Australian Border Force (ABF).

Examples demonstrating ASIO's impact on stakeholder policy development include the following.

Our advice provided context

- ASIO advice and input has informed Office of National Intelligence assessment and published product, including the Prime Minister's Intelligence Daily.
- ASIO Community Contact Program briefing to Home Affairs provided useful context and informed the planning of Home Affairs reporting efforts.

Our advice was relevant and practical

- In the reporting period, ASIO received positive feedback for relevant and practical investigative input which prompted ongoing National Intelligence Community activities related to potential irregular immigrants located in Indonesia.

Our advice influenced decision-making

ASIO advice influenced decision-making and informed partner policy initiatives.

- ASIO contributed to Home Affairs assessment product and threat-prioritisation frameworks, with Home Affairs modifying threat prioritisation matrixes and incorporating our advice directly into its decision-making processes.

Result—impact of ASIO border-related operational activities advice

6. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our advice on countering serious threats to Australia's border integrity, security-sensitive areas or substances had a MEDIUM impact on their decision-making in relation to actions and activities to disrupt and defend against serious threats to Australia's border integrity, security-sensitive areas or substances.			
Target	2020–21	70%; MEDIUM	Outcome	ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 9) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

Stakeholder survey results show 100 per cent of stakeholders surveyed rated ASIO's performance as having a **MEDIUM** or higher impact. ASIO's advice was useful in shaping or informing border-related operational activities and added balance to other lines of reporting; by doing so it directly enhanced Australia's border security.

Additional reporting gathered internally on our border operational–related workflows also demonstrated that ASIO advice had a **MEDIUM** level of impact on stakeholder decision-making. We did this by providing security assessments and other actionable advice to key Australian Government border security partners, including DFAT and Home Affairs portfolio agencies such as the AFP and ABF.

Examples demonstrating ASIO's impact on operational activities include the following.

Our advice provided context and was relevant and practical

ASIO assisted whole-of-government responses to threats to Australia's border integrity. In the reporting period, we continued to provide relevant and practical support to partner agency background-checking services.

- Home Affairs portfolio partners reported that ASIO's processing time for security assessments was well within existing service-level agreements during the reporting period.
- Partners (including AusCheck) reported that ASIO advice has been relevant and practical and provided within existing service-level agreements.

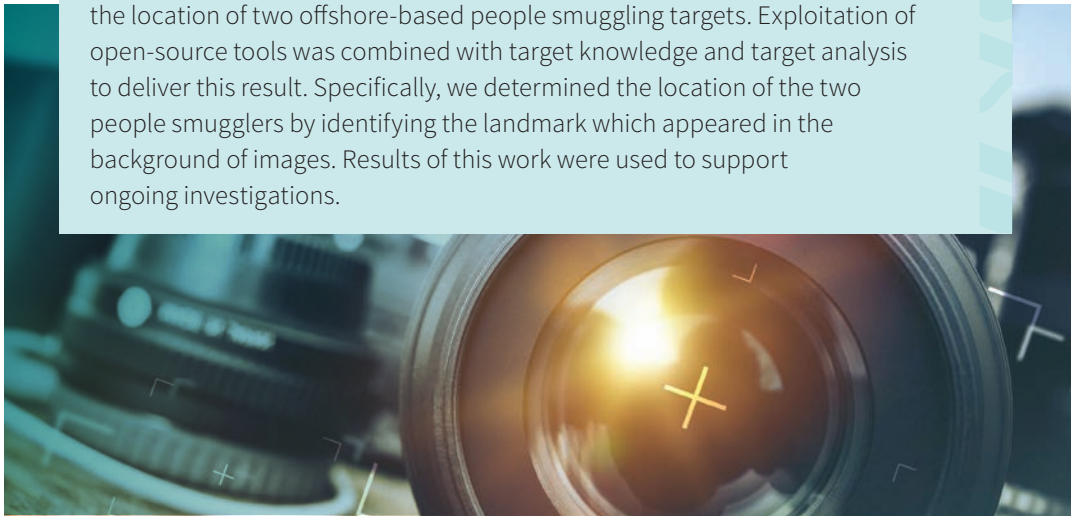
Table 1: Completed visa assessments

Type of entry	2018–19	2019–20	2020–21
Temporary visas	1219	589	506
Permanent residence and citizenship	155	49	24
Onshore protection (air)	32	8	7
Offshore refugee/humanitarian	747	115	43
Illegal maritime arrivals	40	14	4
Other referred caseloads	2121	1740	909
Resolution of national security border alerts	7385	8530	4478
Total	**11 699**	**11 045**	**5971**

- We worked closely with partners to find efficiencies which, combined with reduced travel as a result of COVID-19, resulted in a significantly decreased number of referrals for visa security assessments during the reporting period.
- We issued a number of adverse and qualified assessments, informing stakeholders' decision-making on the issuing or cancelling of visas, or the refusal of citizenship, to mitigate a range of national security risks.

Case study—border security

In March 2021, ASIO and partner agency open-source collaboration identified the location of two offshore-based people smuggling targets. Exploitation of open-source tools was combined with target knowledge and target analysis to deliver this result. Specifically, we determined the location of the two people smugglers by identifying the landmark which appeared in the background of images. Results of this work were used to support ongoing investigations.



Reform program

ASIO is committed to accelerating the delivery of our mission through improvements to our technology. ASIO's reform program will modernise our data analytics and increase the speed and scale of our discovery and investigative work; and deliver reforms across the Organisation to improve effectiveness in our decision-making, resolve threats quickly and drive down risk.

Reform program

Result—ASIO IT service management

7. IT Service Management

Measure	Benchmarking ASIO's maturity for IT service management against an industry standard. Once benchmarked, develop a plan to increase ASIO's maturity for IT service management to the desired level, within the set timeframe.			
Target	2020–21	ESTABLISH BASELINE	Outcome	ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 10) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

A process to benchmark ASIO's IT service management maturity was undertaken, using an industry standard based on the Information Technology Infrastructure Library (ITIL). A Service Management Maturity Assessment (SMMA) model was developed, which will allow ASIO to continue to reassess IT service management maturity on an ongoing basis.

To enable a focused ITIL assessment, customised questions were collated for each of the 10 identified high-priority IT practice areas, including functions such as service request management and IT asset management. The assessment questions were categorised across the dimensions of 'people', 'practices' and 'technology/tools'. Questions across each of these sub-categories were included for all IT practice areas assessed. A number of workshops were also conducted involving representatives with appropriate subject matter knowledge of the IT practice areas.

The outcomes of the SMMA development and workshops provided a targeted assessment of maturity across the priority IT practice areas—establishing a baseline. The maturity assessment report findings informed the development of a high-level roadmap and project proposal. The project aims for progressive, targeted improvements in service delivery that will be sustained beyond the conclusion of the project.

Through benchmarking our IT service management maturity, and developing a plan to increase that level where necessary, ASIO will be better positioned to extract value from our investments in technology to support our mission.

Result—ASIO staff satisfaction with workflow improvements

7. Staff satisfaction with workflow improvements

Measure	The percentage of employees who agree (using a seven-point scale) that: 1. the workflow improvements have led to either (a) a reduction in the manual work previously required of them or (b) the streamlining of duplicative processes; 2. the tool support, developed as part of the workflow improvements, has made it easier for them to resolve issues themselves; and 3. bringing the workflow on-system has provided consistency and visibility to the work done.			
Target	2020–21	50% OF STAFF IN AFFECTED AREA 'SOMEWHAT AGREE' OR HIGHER FOR ALL THREE CATEGORIES	Outcome	ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 10) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

A range of workflow improvements were developed and deployed—via multiple individual projects—throughout the year, targeting focus areas identified through internal consultation.

In parallel with the workflow improvements, a suite of support materials were developed to support users to adopt the changes. These materials included tailored online support such as guides and links to policies and procedures, online discussion forums and targeted workshops.

To measure the benefits delivered by the workflow changes, we assessed staff satisfaction levels through surveys and targeted feedback sessions, both before and after the workflow changes were made. The questions put to stakeholders, while comparable with the measures listed in the *ASIO Corporate Plan 2020–24*, were adjusted to be more relevant and specific to the deployed changes. This approach provided more targeted feedback on the impact of the changes, which will further inform the direction of future workflow changes.

Based on these survey results and stakeholder feedback, there is evidence that the requirement for manual and duplicative work to compile all the information for a required intelligence decision has been measurably reduced, and that overall staff satisfaction with the workflow changes that achieved this is above 50 per cent for staff surveyed.

The user feedback and usage statistics show that the tool support and documentation provided has enhanced users' ability to resolve issues themselves, without seeking additional technical assistance.

Survey results and user feedback have shown that the workflow changes introduced have brought improved consistency and visibility to ASIO processes. The consolidation of data sources has led to a significant uplift in the effectiveness of our analytic processes. Improved data visibility to assist with decision-making and more streamlined processes has resulted in more comprehensive intelligence outcomes.

Overall the workflow changes implemented are assessed to have resulted in measurable workflow improvements, as well as overall staff satisfaction levels above 50 per cent for relevant stakeholder cohorts, across all of the three measures. We assess that we will achieve further improvement over time as the changes become more integrated into ASIO's day-to-day work practices.

Governance and accountability

High levels of public trust are critical to ASIO's operations and the effective and efficient delivery of our purpose. ASIO achieves this through strict compliance with the law, stringent application of policies and procedures, and our active cooperation with external oversight. ASIO is committed to the continual improvement of our enterprise management and governance practices to assure Australians that we pursue our work with integrity and accountability.

Governance and accountability

Result—governance and accountability

9. Compliance framework maturity

Measure	The maturity of ASIO's compliance framework across the Organisation's obligations including, but not limited to, inquiries and investigations, safety and security, and finances.			
Target	2020–21	ESTABLISH BASELINE	Outcome	ACHIEVED
Source	*ASIO Corporate Plan 2020–24* (p. 11) | *PBS 2020–21*, Outcome 1 (Table 2.2)			

In 2020–21, ASIO demonstrated our ongoing commitment to the highest standards of ethics and compliance through maturing our compliance framework and our observance of applicable laws, regulations, rules and policies.

A compliance maturity assessment was undertaken in accordance with the 'Governance and Accountability' performance measure detailed in the *ASIO Corporate Plan 2020–24*.

- ASIO identified a model and measurement scale to assess ASIO's compliance maturity. The compliance maturity model defines the themes and characteristics of compliance at different levels, allowing for a staged progress. Within this model, statements or indicators summarise the themes and characteristics of compliance at each level of maturity.
- The model draws on Australian Standard *Compliance management systems—guidelines* (AS ISO 19600:2015), to define the themes and characteristics of compliance management.
- Stakeholder consultation was conducted to inform the key themes for the compliance maturity assessment, and to define the characteristics and behaviours to demonstrate achievement of the key themes at each given level of maturity. A five level measurement scale was developed to assess ASIO's compliance maturity.
- An initial maturity assessment was conducted utilising evidence-based data and consultation with key stakeholders. This provided a baseline maturity assessment for 2020–21, which has informed the establishment of maturity assessment targets for 2021–22 to ensure continuous improvement.

Invested in its people, practices and technology

Provided influential advice and operational activities

Supported whole-of-government efforts

Enhanced partnerships

Countered terrorism

Countered espionage and foreign interference

Collected intelligence

Provided analysis and security advice on complex visa applications

Analysis of performance

ASIO achieved its purpose during the reporting period through the delivery of outcomes against key priorities. Stakeholders are highly satisfied with their partnerships with ASIO, and there continues to be an overall improvement in the perception of our performance and impact.

ASIO is seen as an organisation that delivers well-considered influential advice and operational activities. Opportunities for improving our partnerships include closer engagement and proactive exchanges of targeted information.

ASIO's security intelligence program contributed to the outcomes of other agencies through security advice, intelligence and services. Our advice to partners within government, the national security community, industry and community sectors in 2020–21 provided the knowledge and understanding to enable them to respond appropriately to security threats.

ASIO countered terrorism and protected Australians from religiously motivated and ideologically motivated violent extremism. ASIO collected intelligence within Australia and overseas, analysed and investigated terrorist threats, and worked with our domestic and overseas partners to protect Australia and Australians from threats to their security. The impact of ASIO's advice and collaborative work is demonstrated by positive stakeholder feedback and successful operational activity.

ASIO countered espionage and foreign interference by delivering targeted effects against foreign intelligence services seeking to covertly influence, undermine or conduct espionage against Australia's government information, political systems, military capabilities, non-military strategic assets and community. ASIO collection and investigations helped discover and understand the nature of the threats against Australia, our advice hardened vulnerable sectors, and we collaborated with partners to disrupt and deter those harming our national interests.

ASIO supported whole-of-government efforts to protect Australia's border integrity by providing analysis and security advice on complex visa applications and other movements of goods and people, to assist partners to maintain the integrity of Australia's border protection programs.

ASIO continued to invest in its people, practices and technology. Ensuring the safety of our staff in a COVID-19 environment, ASIO adopted a range of strategies to sustain coverage of high-priority targets related to our counter-terrorism and counter–espionage and foreign interference missions.

ASIO made progress in the delivery of improvements to the technology and systems that underpin our mission delivery. The reform program is a multi-year initiative, and we expect to deliver further improvements as the program evolves.

The effectiveness of our partnerships has contributed significantly to the achievement of our purpose. ASIO is seen as a high-quality and valued partner worthy of stakeholder investment and offering unique value. Ongoing engagements, high levels of performance, and a commitment to enhanced partnerships has and will continue to support the achievement of our purpose.

Report on financial performance

Financial performance

The COVID-19 pandemic continued to have an impact on the delivery of ASIO's activities for the 2020–21 financial year, resulting in less expenditure than initially planned. The financial statements report an $82.2 million operating deficit compared with $90.1 million operating deficit in 2019–20. ASIO's 2020–21 operating funding from Government was $455.2 million compared to $473.0 million in 2019–20. In 2020–21 ASIO incurred $142.0 million in depreciation and amortisation expenses (including for the right-of-use leased assets) noting that the Australian Government does not provide operating funding for these expenses. ASIO also incurred $34.2 million in principal repayments for leased assets reflecting the implementation of AASB 16 Leases which became effective on 1 July 2019. After adjusting for these items, the 2020–21 operating result is a surplus of $25.6 million compared to $17.1 million in 2019–20.

ASIO commenced a modest self-funded program of reforms to accelerate the delivery of our mission through improvements to our technology. This reform work will continue into 2021–22.

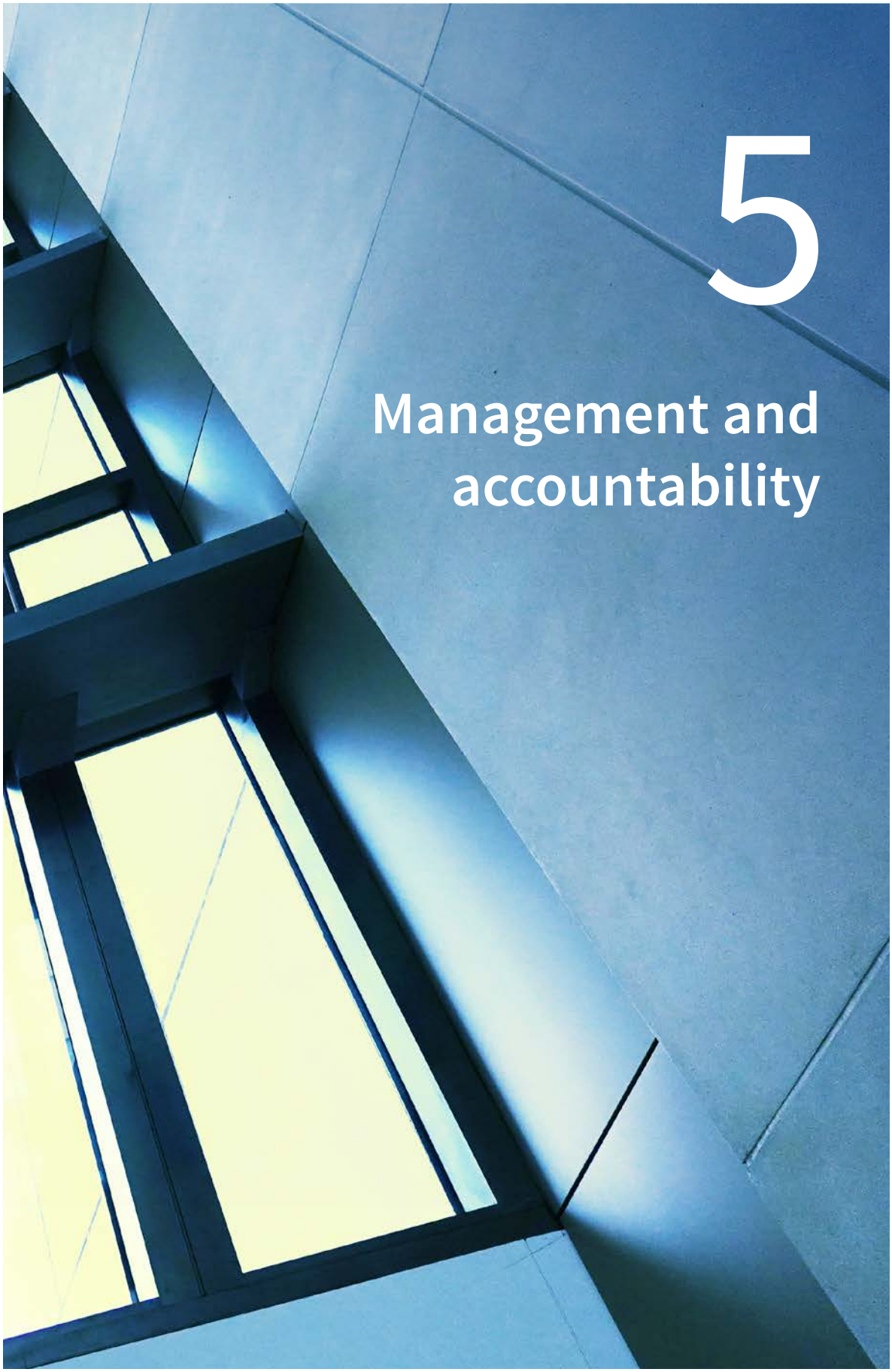
ASIO's 2020–21 departmental capital budget funding was $82.3 million, compared with $61.3 million the previous financial year. This funding has been applied to the necessary development, enhancement and replacement of assets to support ASIO's operational effectiveness in the increasingly fluid security and technology environments. In 2020–21 ASIO received $10.5 million as an equity injection compared with $10.9 million in 2019–20.

ASIO has continued to identify and implement efficiencies across its operations and contribute to Australian Government savings measures.

ASIO's complete financial results for 2020–21 are available in the financial statements in this report.

A table summarising ASIO's total resources for 2020–21 is provided at **Appendix A**.

Our total expenses by outcome for this reporting period are at **Appendix B**.



5

Management and accountability

Corporate governance

Our governance processes guide us in achieving our mission and meeting public expectations of probity, accountability and transparency.

The Director-General of Security is the accountable authority for ASIO under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The Director-General is supported by a number of corporate governance committees, including ASIO's peak governing body (the Executive Committee); two internal advisory committees (the Security and Compliance Committee, and the Capability and Investment Committee); and an independent advisory committee (the Audit and Risk Committee).

In 2020–21, ASIO refined its enterprise management and governance practices by maturing:

- ASIO's enterprise risk framework, supported by a new risk appetite and tolerance statement reflecting contemporary risks; and
- ASIO's business continuity framework, to ensure the Organisation is positioned to sustain high-priority operations in the event of a significant disruption.

Executive Committee

The Executive Committee advises the Director-General on matters requiring executive decision-making. The Executive Committee's purpose is to provide oversight of all ASIO activities, including setting the strategic direction for the Organisation, setting priorities for the Organisation's intelligence mission, and reviewing the Organisation's performance against those priorities. The Executive Committee also sets and reviews the Organisation's risk appetite and tolerance, determines whether ASIO's overall level of risk is acceptable, and considers whether the risk management framework remains effective.

Security and Compliance Committee

The Security and Compliance Committee, chaired by the Deputy Director-General Intelligence Service Delivery, makes recommendations to the Executive Committee on significant security and compliance matters relating to or impacting on ASIO, including the successful delivery of ASIO's strategic objectives and management of enterprise risk.

Capability and Investment Committee

The Capability and Investment Committee, chaired by the Deputy Director-General Enterprise Service Delivery, makes recommendations to the Executive Committee on significant matters related to organisational capability and investment, and ensures capability is aligned to ASIO's strategic objectives.

Figure 2: ASIO's governance framework

ASIO's response to COVID-19

ASIO continues to adopt a range of strategies to sustain coverage of high-priority targets related to our counter-terrorism and counter–espionage and foreign interference missions, while ensuring the safety of our staff.

Our response to COVID-19 has been overseen by the ASIO Crisis Management Team (CMT), chaired by the Deputy Director-General Enterprise Service Delivery. The CMT has managed the Organisation's response to the pandemic, ensuring that the Organisation complied with public health directions, while sustaining high priority operations. The CMT has also overseen the implementation of adaptive working arrangements and COVID-safe measures to minimise the impact to operations as the nature of the pandemic evolves.

ASIO's response to COVID-19 also prompted the review and maturation of our business continuity framework, ensuring we are well positioned to respond to current and future disruptions to our business.

External scrutiny

Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) performs a key role in ASIO's independent oversight and accountability framework by providing assurance to the Australian community about ASIO's performance of its functions.

The PJCIS's remit includes overseeing ASIO's administration and expenditure, reviewing national security bills, and ensuring national security legislation remains necessary, proportionate and effective.

In 2020–21, ASIO provided a written submission to the PJCIS Review of Administration and Expenditure No. 19 (2019–20). Beyond administration and expenditure, ASIO also contributed, either directly or as part of a Home Affairs portfolio submission, to a number of other PJCIS reviews and inquiries, including:

- the review of the ASIO Amendment Bill 2020;
- the review of the amendments made by the *Telecommunications and Other Legislation Amendments (Assistance and Access) Act 2018*;
- the review of the Counter-Terrorism Legislation Amendment (High Risk Terrorist Offenders) Bill 2020;
- the inquiry into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020;
- the review of the Migration and Citizenship Legislation Amendment (Strengthening Information Provisions) Bill 2020;
- the review of the 'declared area' provisions;
- the review of Australian Federal Police powers;
- the statutory review of part 14 of the *Telecommunications Act 1997*;
- reviews of the listing and relisting of terrorist organisations;
- the inquiry into extremist movements and radicalism in Australia; and
- the inquiry into national security risks affecting the Australian higher education and research sector.

Other parliamentary committee inquiries

ASIO provides submissions to other parliamentary committees, as appropriate. In 2020–21, ASIO contributed, either directly or as part of a Home Affairs portfolio submission, to:

- the Senate Foreign Affairs, Defence and Trade References Committee Inquiry into the Issues Facing Diaspora Communities in Australia; and
- the Joint Standing Committee on Electoral Matters Inquiry on the Future Conduct of Elections Operating during Times of Emergency Situations.

Senate Legal and Constitutional Affairs Committee

ASIO appeared before the Senate Legal and Constitutional Affairs Committee as part of the Senate Estimates process on 20 October 2020, 22 March 2021, 14 April 2021 and 25 May 2021.

ASIO's evidence to the committee can be found in the estimates Hansard for those days (refer to www.aph.gov.au/Parliamentary_Business/Senate_Estimates and navigate to the relevant hearing).

Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) assists ministers to oversee and review the activities of intelligence agencies for legality and propriety.

The IGIS performs this function through inspections, inquiries, and investigations into complaints. The IGIS is also required to assist the government to assure the public and the parliament that Commonwealth intelligence and security matters are open to scrutiny.

The IGIS retains statutory powers akin to those of a standing royal commission.

Meeting our legal obligations and embodying the highest ethical standards is critical to maintaining the trust of the Australian public and our ongoing effectiveness as Australia's security intelligence organisation.

Every ASIO officer is responsible for complying with our legislated requirements, the Minister's Guidelines for ASIO, and associated internal policies and procedures. Central to this is acting with integrity and ensuring proportionality in all our work.

During 2020–21 the IGIS regularly inspected activities across our operational functions, and investigated a small number of complaints received by the Office.

During the reporting period, ASIO completed its implementation of recommendations arising from two inquiries undertaken by the IGIS in the 2018–19 reporting period.

ASIO has adopted in full the two recommendations from the IGIS's preliminary inquiry into the application of national security classifications undertaken this reporting period, and has also addressed other issues as raised by the IGIS.

Independent National Security Legislation Monitor

The Independent National Security Legislation Monitor (INSLM) reviews the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation, and reports to the Prime Minister and parliament on an ongoing basis.

The INSLM considers whether the laws contain appropriate safeguards to protect individuals' rights, remain proportionate to threats of terrorism or national security, and remain necessary. The Prime Minister may also refer a counter-terrorism or national security matter to the INSLM, either at the INSLM's suggestion or on the Prime Minister's initiative, under the Act.

During 2020–21 ASIO appeared at a public hearing to give evidence to the review of the operation of section 22 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* as it applies in the 'Alan Johns' matter (a pseudonym).

Independent Reviewer of Adverse Security Assessments

The Independent Reviewer of Adverse Security Assessments (Independent Reviewer) reviews adverse ASIO security assessments that impact individuals who are in immigration detention and who have been found by Home Affairs to be owed protection under international law.

The Independent Reviewer conducts a primary review of each adverse security assessment. For eligible individuals, these assessments are periodically reviewed—every 12 months—for the duration of the adverse assessment.

Appendix I provides the Independent Reviewer's annual report for the current reporting period.

Compliance

Ethical behaviour and integrity are core values of the Organisation, and are essential to sustaining the confidence and trust of the parliament and the Australian people. We earn this confidence through strict compliance with the law, stringent application of policies and procedures, and active cooperation with external oversight bodies.

Centralised internal audit and compliance functions are key components of ASIO's approach to corporate governance. These provide assurance to the Director-General that our risk, control and compliance measures ensure our resources are used efficiently, effectively and ethically. This includes taking all reasonable steps to prevent, deter and address fraud. These efforts also serve to ensure ASIO is positioned to meet current and future security challenges.

Internal audit function

ASIO's internal audit function is designed to add value and improve our operations and service delivery. By applying a systematic and disciplined approach to evaluation and advice, the function supports effective and efficient internal control and governance frameworks.

Subject to security policies and operational considerations, our internal audit function has unrestricted access to all ASIO premises, work areas, documentation and information necessary to meet its responsibilities.

During the reporting period, ASIO undertook a program of compliance audits and performance reviews.

Compliance function

ASIO's compliance function is focused on ensuring the Organisation continues to demonstrate its commitment to the highest standards of ethics and compliance with all applicable laws, regulations, rules and policies.

During the reporting period, our centralised compliance function and internal assurance frameworks continued to mature.

ASIO Audit and Risk Committee

The ASIO Audit and Risk Committee is an independent advisory body, responsible for providing independent assurance and advice to the Director-General and the Executive Committee on ASIO's risk oversight and management, financial and performance reporting responsibilities, and systems of internal control.

The committee operates under a charter which sets out its functions and responsibilities in accordance with section 45 of the PGPA Act and section 17 of the Public Governance Performance and Accountability Rule.[1]

[1] Consistent with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the annual report has not provided a direct electronic address for the charter determining the function of the ASIO Audit and Risk Committee.

Under the Audit and Risk Committee's charter, the committee has four external members, including an external chair, as well as observers from the Australian National Audit Office.[2] The audit committee members have a broad range of appropriate qualifications, knowledge, skills and experience relevant to the operations of ASIO. This includes at least one member with accounting or related financial management experience, and an understanding of accounting and auditing standards in a public sector environment. On appointment, committee members receive an induction briefing on ASIO governance and operations.

During this reporting period, the committee met five times (four quarterly meetings and an extraordinary meeting convened for the financial statements review). Each meeting had a quorum, with all members attending two meetings, and all but one attending the remaining three.

Fraud control and management

ASIO has zero tolerance for fraudulent behaviour. ASIO treats both suspected and actual fraud seriously and takes all reasonable measures to prevent, detect and investigate fraudulent behaviour. The *ASIO Fraud Control Plan 2019–21* documents our approach to fraud awareness, prevention, detection, reporting and investigation, and our commitment to ensuring efficient, effective and ethical use of resources—including the information and data we collect, and the resources we receive from government. Our fraud prevention measures are in line with the *Commonwealth Fraud Control Framework 2017*.

During the reporting period, we conducted fraud pressure-testing on a sample of countermeasures (also known as controls) identified in our Fraud Risk Assessment. This allowed us to identify fraud vulnerabilities and determine the effectiveness of our countermeasures.

As part of this framework, all staff must complete mandatory eLearning on ethics and accountability, including modules on fraud, during induction and then at least every three years thereafter.

The *ASIO Fraud Strategy Statement 2021* (www.asio.gov.au/asio-fraud-strategy-statement.html) provides further information on our fraud control and management arrangements.

[2] Consistent with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the annual report has not provided membership and remuneration details.

Significant legal matters affecting ASIO's business

In 2020–21 ASIO was involved in legal proceedings in courts and tribunals. Matters included terrorism prosecutions, judicial and merits reviews of security assessments, coronial inquests and civil lawsuits.

Administrative Appeals Tribunals

ASIO was involved in proceedings before the Administrative Appeals Tribunal (AAT) in the 2020–21 reporting period. Most of these proceedings were reviews of ASIO security assessments. Three matters related to reviews of National Archives access decisions involving ASIO material.

AAT decisions are reported on the Australasian Legal Information Institute (AustLII) website, www.austlii.edu.au.

Tribunal reviews—security assessments

Over the 2020–21 reporting period, there were 12 AAT reviews of ASIO adverse security assessments, and two AAT reviews of ASIO qualified security assessments. These ASIO security assessments related to eligibility for passports, visas, security clearances and citizenship.

Of these 14 matters:

- one decision was handed down, affirming the adverse security assessment that was the subject of the review;
- one assessment was remitted to ASIO for a new assessment to be prepared. This assessment remains under consideration at the end of the reporting period;
- three matters were heard, and decisions remain reserved at the end of the reporting period;
- two matters were withdrawn; and
- seven matters are pending before the AAT at the end of this reporting period.

Tribunal reviews—archives matters

Over this reporting period, ASIO assisted the AAT in three reviews of National Archives access decisions in which exemptions had been claimed to protect ASIO material from release.

Criminal prosecutions

In collaboration with our law enforcement partners and prosecuting authorities—and with appropriate protections—ASIO provided information for use as evidence to prosecutions, and responded to subpoenas and disclosure requests.

Federal and High Court reviews—security assessments

ASIO was involved in Federal and High Court proceedings, both as a respondent in security assessment reviews and as an interested third party in other proceedings. We worked closely with other stakeholders to manage the collective Commonwealth interest.

Management of human resources

Current workplace agreement

ASIO's terms and conditions of employment are set out in a determination approved by the Director-General under the ASIO Act. During the reporting period, 67 Senior Executive Service (SES) employees and 2059 non-SES employees were covered by the determination.

A wage increase under the current determination took effect from 29 October 2020 for non-SES employees, following a six-month wage deferral consistent with Australian Government policy. SES employees did not receive a wage increase during the period.

The Executive Vehicle Scheme is available to SES officers and employees at the AEE3 classification. Under the scheme, eligible employees are provided with an executive vehicle unless the employee elects to be paid cash in lieu of the executive vehicle.

The salary ranges available for employees by classification level are shown at **Appendix D**.

Performance management

All ASIO employees participated in the 2020–21 performance management cycle, consistent with policy requirements.

To further strengthen ASIO's commitment to high performance, a range of enhancements were made to the 2020–21 Performance Agreement to better capture accountabilities, outcomes and behaviours, and encompass corporate contributions and agreed flexible working arrangements.

Consistent with ASIO's commitment to support and develop our leaders, ASIO has introduced manager-once-removed feedback for executive and SES officers, as part of the performance framework. This involves managers gathering feedback about their direct reports from team members or internal stakeholders and then using that feedback to help focus ongoing leadership development.

People strategy

ASIO has adopted a five-year Workforce Plan to ensure the Organisation is well positioned to meet future workforce challenges. The three key areas of focus in the plan are capability, efficiency and engagement.

Actions completed in the first year of the plan included:

- delivering an updated and integrated People Capability Framework;
- conducting an all-staff survey; and
- commencing drafting a suite of job role profiles.

These deliverables support professional development, retention and staff engagement.

Diversity and inclusion

ASIO continues to make positive progress towards increasing the diversity of its workforce and ensuring the workplace is inclusive. Guided by our *Diversity and Inclusion Strategy 2021–24*, our progress has been supported by ASIO's Diversity and Inclusion Council and Senior Executive Champions. Key achievements included:

- the release of ASIO's *Diversity and Inclusion Strategy 2021–24*;
- the achievement of gender balance in our SES; and
- the launch of our first affirmative (Indigenous) measures recruitment round.

The objectives of our strategy focus on embedding diversity and inclusion in everything we do, and ensuring that our people reflect the community we protect. We continue to leverage the diversity of our workforce to achieve mission outcomes and to ensure that our employees feel empowered to bring their whole selves to work.

ASIO has continued to work collaboratively across the National Intelligence Community in diversity and inclusion. ASIO has led several initiatives and days of significance, bringing our National Intelligence Community partners together in recognition of our shared diversity objectives.

Statistics on the diversity of our workforce are provided at **Appendix E**.

ASIO has seven staff-led networks which play an important role in contributing to its diverse and inclusive culture. The networks provide support and empower staff to initiate organisational change to achieve ASIO's diversity and inclusion goals.

ASIO's diversity networks are championed by members of the SES who help to achieve our diversity objectives by:

- providing guidance and support directly to the networks; and
- working across the senior levels of the Organisation.

Diversity networks

aGENda

ASIO's gender-equity network promotes equal opportunity for ASIO's workforce, regardless of gender. The aGENda network organises events and initiatives to ensure gender equity considerations continue to shape the corporate agenda.

ASIOpen

ASIO's gender diverse and sexually diverse network promotes an inclusive workplace culture and supports gender diverse and sexually diverse employees to be open and authentic in the workplace.

CapABILITY

ASIO's CapABILITY network represents staff who experience any form of physical or mental health issue, neurodiversity or caring responsibilities.

Introverts

ASIO's introverts network contributes to all staff being heard, recognised and valued for their contributions, regardless of how introverted or extroverted they are.

Mozaik

Mozaik—ASIO's cultural diversity network—fosters collaboration across ASIO's workforce to develop tangible work programs to remove potential barriers to acceptance and opportunity.

Mudyi

The Mudyi Network seeks to raise awareness and appreciation of Indigenous culture and drive corporate initiatives aimed at improving the workplace experience for Indigenous people.

Parents Network

This network is for ASIO staff who are parents, or about to become parents. It helps them while they are on leave and as they return to work to navigate flexible and part-time working arrangements.

ASIO Ombudsman

The ASIO Ombudsman is an external service provider who works to resolve employee issues or concerns impartially and informally through advice, consultation and mediation.

During the reporting year, the ASIO Ombudsman supported employees and line managers through:

- informal discussions;
- reviews of policy documents; and
- information-sharing, such as best-practice policy and research papers.

In addition, the following formal engagements occurred:

- seven staff requests on topics such as recruitment and career path options;
- one health review;
- two discussions with staff networks;
- three inquiries into staff concerns; and
- two meetings with inter-agency stakeholders.

In 2020–21 the ASIO Ombudsman did not participate in any work related to public interest disclosures.

Asset management

The Organisation's governance framework for managing assets so that asset balances in the financial statements are accurately reported includes:

- asset investment and replacement, through setting an annual budget that reflects both government priorities and ongoing business requirements. The budget is monitored monthly and reviewed regularly during the year to ensure planned expenditure reflects business requirements;
- undertaking a rolling annual stocktake, impairment review and useful life expectancy review to update and verify the accuracy of asset records;
- conducting fair-value measurement through two-yearly revaluations of all tangible assets, which is completed by qualified external valuers. Materiality review is undertaken in the years between valuations; and
- maintaining property, plant and equipment assets through maintenance programs.

Additional information on the value, acquisition and disposal of assets is available in the 2020–21 financial statements of this report.

Purchasing

During 2020–21 ASIO adhered to the Commonwealth Procurement Rules (CPR) and associated policy and guidelines. ASIO's compliance was monitored by the Audit and Risk Committee as well as the Security and Compliance Committee. No significant issues were identified, and overall compliance was acceptable.

Consultants

During the 2020–21 reporting period, ASIO entered into 30 new consultancy contracts, involving total actual expenditure of $2 589 896 (GST-inclusive). In addition, four ongoing consultancy contracts were active during the reporting period, involving total actual expenditure of $144 592 (GST-inclusive).

Table 2: Expenditure on reportable consultancy contracts for the current reporting period (2020–21)

	Total
Number of new contracts entered into during the period	30
Total actual expenditure on new contracts during the period (GST-inclusive)	$2 589 896
Number of ongoing contracts entered into during a previous period	4
Total actual expenditure on ongoing contracts during the period (GST-inclusive)	$144 592

ASIO applied the CPR and Department of Finance guidance when selecting and engaging consultants. We also followed internal policy and associated procedures on identifying and determining the nature of a contract. This ensured that we used appropriate methods for engaging and contracting consultants.

ASIO engaged consultants when we needed professional, independent and expert advice or services that were not available within the Organisation.

In the 2020–21 reporting period we also entered into 474 new non-consultancy contracts involving total actual expenditure of $91 328 873 (GST-inclusive). In addition, 209 ongoing non-consultancy contracts were active during the reporting period, involving total actual expenditure of $59 562 499 (GST-inclusive).

Table 3: Expenditure on reportable non-consultancy contracts for the current reporting period (2020–21)

	Total
Number of new contracts entered into during the period	474
Total actual expenditure on new contracts during the period (GST-inclusive)	$91 328 873
Number of ongoing contracts that were entered into during a previous period	209
Total actual expenditure on ongoing contracts during the period (GST-inclusive)	$59 562 499

Annual reports contain information about actual expenditure on contracts for consultancies and non-consultancies; information on the value of contracts is available on the AusTender website. However, we are not required to publish information on the AusTender website, in line with authorised exemptions to avoid prejudice to our national security activities. A list of consultancy and non-consultancy contracts to the value of $10 000 or more during this reporting period, and the total value of each of those contracts over the life of each contract, is available to the PJCIS on request, which oversees our administration and expenditure.

Australian National Audit Office access clauses

During this reporting period, ASIO did not enter into any contracts valued at $100 000 or more that did not provide the Auditor-General with access to the contractor's premises.

Exempt contracts

The Director-General has applied measures necessary to protect national security which exempt ASIO from publishing details of contract arrangements, including standing offers, in accordance with clause 2.6 of the CPR. Details of our arrangements, contracts and standing offers are available to the PJCIS on request.

Procurement initiatives to support small business

Throughout 2020–21 ASIO adhered to the CPR and associated policy and guidelines. ASIO's compliance was monitored through the Audit and Risk Committee and the Security and Compliance Committee. No significant issues were identified, and overall compliance was acceptable.

ASIO supports small business participation in the Australian Government procurement market. Small and medium enterprises (SME) and small enterprise participation statistics are available on the Department of Finance's website at www.finance.gov.au.

Our procurement practices to support SME include:

- standardising contracts and approach-to-market templates, using clear and simple language;
- ensuring information is easily accessible through the electronic advertisement of business opportunities and electronic submission for responses; and
- using electronic systems to facilitate the Department of Finance's Procurement On-Time Payment Policy for Small Business, including payment cards.

ASIO recognises the importance of ensuring that small businesses are paid on time. The results of the survey of Australian Government Payments to Small Business are available at www.finance.gov.au/government/procurement/statistics-australian-government-procurement-contracts.

Other mandatory information

Advertising and market research

In the financial year 2020–21, ASIO expended $314 183 on marketing and advertising campaigns. Further information on these advertising campaigns is available at www.asio.gov.au and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website (see also **Appendix G**).

ASIO does not fall within the definition of agencies covered by the reporting requirements of section 311A of the *Commonwealth Electoral Act 1918*.

Disability reporting

The *National Disability Strategy 2010–2020* is Australia's overarching framework for disability reform. It acts to ensure the principles underpinning the United Nations Convention on the Rights of Persons with Disabilities are incorporated into Australia's policies and programs that affect people with disability, their families and carers.

All levels of government will continue to be held accountable for the implementation of the strategy through biennial progress reporting to the Council of Australian Governments. Progress reports can be found at the Department of Social Services website, www.dss.gov.au.

Appendix E of ASIO's annual report provides information on the diversity of our workforce, including statistics on people with a disability. The annual report is also available at www.asio.gov.au.

Commonwealth Child Safe Framework—statement of compliance

ASIO has a strong commitment to child safety, and protecting and safeguarding children, while promoting and maintaining a culture that provides a safe environment for children.

ASIO's purpose is to protect Australia and Australians from threats to their security. In meeting this purpose, ASIO has occasional contact with minors, including direct and indirect contact.

An annual review of organisational child-related risks has been undertaken to ensure that existing and emerging risks to children are identified and that appropriate mitigation strategies are developed. The overall risk rating of the safety of children and young people during operations in 2020–21 is medium. By complying with the requirements of the Commonwealth Child Safe Framework (CCSF) and identifying and controlling these risks, the risk to children is mitigated.

ASIO's activities are consistent with each of the four requirements of the CCSF.

ASIO's operational and investigative activity involving children is managed through the application of laws and policies to support children's physical and psychological safety; the maintenance of a workforce that is appropriately trained, qualified and compliant with mandatory obligations; and the effective identification, reporting and management of child-related incidents. In addition, there are strong safeguards embedded in legislation relating to the compulsory questioning of minors under the ASIO Act.

Staff are aware of the sensitivities that apply when working with children and have access to specialist advice as required.

To further strengthen ASIO's compliance with the CCSF, ASIO has conducted an audit to understand and manage risks related to activities involving child-related work. This work will be used to inform further initiatives, including the review and refinement of training modules and policy.

All ASIO's activities are subject to oversight by the IGIS, who is responsible for reviewing the activities of intelligence agencies for legality, propriety and consistency with human rights.

Archives Act 1983

ASIO is an exempt agency under the *Freedom of Information Act 1982* but is subject to the release of records under the *Archives Act 1983* (Archives Act). This provides for public access to Commonwealth records in the 'open period'. In accordance with changes to the Archives Act in 2010, the open period has transitioned from 30 to 20 years. The current open period covers all Commonwealth records created before 2001. ASIO works closely with the National Archives of Australia to facilitate access to ASIO records.

During the reporting period, ASIO received 537 requests for access to ASIO records, a significant (60 per cent) increase in requests compared with the previous reporting period.

In 2020–21, ASIO completed a total of 538 requests, equating to 47 913 pages requiring assessment.

Most requests (79 per cent) were completed within the 90-business-day legislative time frame, a significant increase compared with 59 per cent in the previous period.

The increase in completions in the reporting period is due to:

- the completion of a large number of small requests; and
- the completion of an increased number of longstanding cases.

Table 4: Access to ASIO records

	2018–19	2019–20	2020–21
Applications for record access	344	334	537
Requests completed	410	399	538
Pages assessed	57 783	72 820	47 913
Percentage of requests completed within 90 days	60%	59%	79%

Australian Security Intelligence Organisation Act 1979

ASIO is required by section 94 of the ASIO Act to include in its annual report, details on its use of questioning warrants; special intelligence operation authorities; authorisations for access to telecommunications data; technical assistance requests, technical assistance notices and technical capability notices; and special powers under warrant.

The statement on questioning warrants is provided at **Appendix J**. To ensure compliance with the determination made by the Minister for Finance under section 105D of the PGPA Act, and to avoid prejudice to ASIO's activities, **Appendix L** relating to special intelligence operation authorities, **Appendix M** relating to telecommunications data access authorisations, **Appendix N** relating to Telecommunications and Other Legislation Amendment (TOLA) authorisations and **Appendix O** relating to use of special powers under warrant have been removed from the annual report tabled in parliament.

These classified appendices are provided separately to ASIO's minister and, as required by the ASIO Act, to the Leader of the Opposition. Copies of the classified appendices will also be provided to the Attorney-General, the IGIS, and the INSLM.

Appendix M relating to telecommunications data access authorisations will also be provided to the PJCIS.

Work Health and Safety Act 2011

Schedule 2, part 4 of the *Work Health and Safety Act 2011* requires non-corporate Commonwealth entities to include in their annual reports information on health and safety outcomes and initiatives taken during the reporting period to ensure the health, safety and welfare of workers who carry out work for them.

Our report for 2020–21 is provided at **Appendix F**.

Commonwealth Electoral Act 1918—advertising and market research

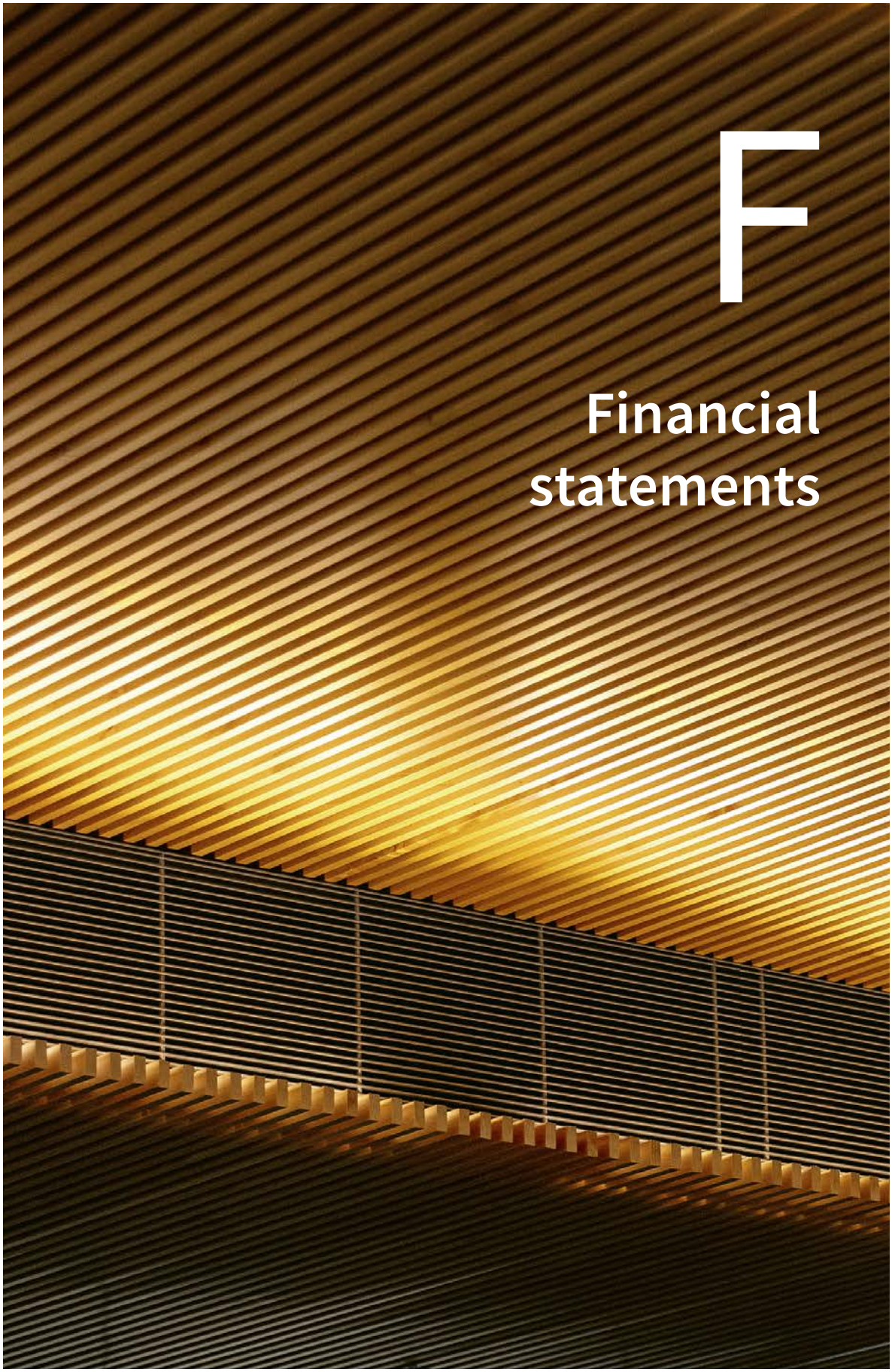
Section 311A of the *Commonwealth Electoral Act 1918* requires annual reporting by each Commonwealth department on amounts paid by, or on behalf of, the Commonwealth department for advertising and market research.

Our report for 2020–21 is provided at **Appendix G**.

Environment Protection and Biodiversity Conservation Act 1999

Section 516A of the *Environment Protection and Biodiversity Conservation Act 1999* requires Commonwealth entities to report on how the activities of the entity during the period accorded with the principles of ecologically sustainable development.

Our report for 2020–21 is provided at **Appendix H**.



F

Financial statements

CONTENTS

Due to rounding, figures presented throughout these financial statements may not add precisely to the totals provided.

Australian National Audit Office

INDEPENDENT AUDITOR'S REPORT

To the Minister for Home Affairs

Opinion

In my opinion, the financial statements of the Australian Security Intelligence Organisation (the Entity) for the year ended 30 June 2021:

(a) comply with the:

- Australian Accounting Standards – Reduced Disclosure Requirements; and
- *Public Governance, Performance and Accountability (Financial Reporting) Rule 2015*

as amended by section 105 D of the *Public Governance, Performance and Accountability Act 2013.*

(b) present fairly the financial position of the Entity as at 30 June 2021 and its financial performance and cash flows for the year then ended in accordance with the requirements of section 105 D of the *Public Governance, Performance and Accountability 2013*.

The financial statements of the Entity, which I have audited, comprise the following as at 30 June 2021 and for the year then ended:

- Statement by the Director-General of Security;
- Statement of Comprehensive Income;
- Statement of Financial Position;
- Statement of Changes in Equity;
- Cash Flow Statement; and
- Notes to the financial statements, comprising a summary of significant accounting policies and other explanatory information.

Basis for opinion

I conducted my audit in accordance with the Australian National Audit Office Auditing Standards, which incorporate the Australian Auditing Standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the Entity in accordance with the relevant ethical requirements for financial statement audits conducted by the Auditor-General and his delegates. These include the relevant independence requirements of the Accounting Professional and Ethical Standards Board's APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)* (the Code) to the extent that they are not in conflict with the *Auditor-General Act 1997*. I have also fulfilled my other responsibilities in accordance with the Code. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

Accountable Authority's responsibility for the financial statements

As the Accountable Authority of the Entity, the Director-General of Security is responsible under the *Public Governance, Performance and Accountability Act 2013* (the Act) for the preparation and fair presentation of annual financial statements that comply with Australian Accounting Standards – Reduced Disclosure Requirements and the rules made under the Act. The Director-General of Security is also responsible for such internal control as the Director-General of Security determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

GPO Box 707, Canberra ACT 2601
38 Sydney Avenue, Forrest ACT 2603
Phone (02) 6203 7300

In preparing the financial statements, the Director-General of Security is responsible for assessing the ability of the Entity to continue as a going concern, taking into account whether the Entity's operations will cease as a result of an administrative restructure or for any other reason. The Director-General of Security is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the assessment indicates that it is not appropriate.

Auditor's responsibilities for the audit of the financial statements

My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with the Australian National Audit Office Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

As part of an audit in accordance with the Australian National Audit Office Auditing Standards, I exercise professional judgement and maintain professional scepticism throughout the audit. I also:

- identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control;
- obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Entity's internal control;
- evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Accountable Authority;
- conclude on the appropriateness of the Accountable Authority's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Entity's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the Entity to cease to continue as a going concern; and
- evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with the Accountable Authority regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

Australian National Audit Office

Rebecca Reilly
Executive Director

Delegate of the Auditor-General

Canberra
25 August 2021

STATEMENT BY THE DIRECTOR-GENERAL OF SECURITY

In my opinion, the attached financial statements for the year ended 30 June 2021 comply with subsection 42(2) of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and are based on properly maintained financial records as per subsection 41(2) of the PGPA Act.

In my opinion, at the date of this statement, there are reasonable grounds to believe that ASIO will be able to pay its debts as and when they fall due.

Mike Burgess
Director-General of Security

25 August 2021

STATEMENT OF COMPREHENSIVE INCOME
for the period ended 30 June 2021

	Notes	2021 $'000	Original budget 2021 $'000	2020 $'000
EXPENSES				
Employee benefits	1.1.A	265 262	280 912	287 088
Suppliers	1.1.B	137 441	152 642	151 999
Depreciation and amortisation	2.2.A	142 023	158 648	139 109
Finance costs	1.1.C	8029	9953	8688
Write-down and impairment of other assets	1.1.D	1316	-	425
TOTAL EXPENSES		**554 071**	**602 155**	**587 309**
OWN-SOURCE INCOME				
Revenue				
Sale of services	1.2.A	9266	22 314	18 019
Other revenue	1.2.B	7016	1806	6141
Gains		369	145	61
TOTAL OWN-SOURCE INCOME		**16 651**	**24 265**	**24 221**
Net cost of services		***(537 420)***	***(577 890)***	***(563 088)***
REVENUE FROM GOVERNMENT	3.1	**455 198**	**465 178**	**473 011**
DEFICIT ON CONTINUING OPERATIONS		**(82 222)**	**(112 712)**	**(90 077)**
OTHER COMPREHENSIVE INCOME				
Changes in Asset Revaluation Reserve		-	-	20 516
TOTAL COMPREHENSIVE LOSS		**(82 222)**	**(112 712)**	**(69 561)**

The above statement should be read in conjunction with the accompanying notes.

STATEMENT OF FINANCIAL POSITION as at 30 June 2021

	Notes	2021 $'000	Original budget 2021 $'000	2020 $'000
ASSETS				
Financial assets				
Cash and cash equivalents		13 787	15 247	16 260
Trade and other receivables	2.1.A	141 790	90 744	110 029
Accrued revenue		493	652	602
Amortisation of subleased right-of-use assets income		1679	-	1441
Total financial assets		***157 749***	***106 643***	***128 332***
Non-financial assets				
Prepayments		31 157	36 646	34 748
Land and buildings	2.2.A	678 175	725 305	736 228
Property, plant, equipment and computer software	2.2.A	214 783	233 661	213 740
Total non-financial assets		***924 115***	***995 612***	***984 717***
TOTAL ASSETS		**1 081 864**	**1 102 255**	**1 113 049**
LIABILITIES				
Payables				
Suppliers	2.3.A	7526	9004	9991
Other payables	2.3.B	7006	14 695	12 420
Total payables		***14 532***	***23 699***	***22 411***
Interest bearing liabilities				
Leases	2.4.A	587 065	638 483	618 532
Total interest bearing liabilities		***587 065***	***638 483***	***618 532***
Provisions				
Employee provisions	2.5.A	93 030	95 063	96 545
Restoration obligations	2.5.B	8273	6649	7225
Other provisions		132	-	-
Total provisions		***101 435***	***101 712***	***103 770***
TOTAL LIABILITIES		**703 032**	**763 894**	**744 713**
NET ASSETS		**378 832**	**338 361**	**368 336**

STATEMENT OF FINANCIAL POSITION as at 30 June 2021 (continued)

	Notes	2021 $'000	Original budget 2021 $'000	2020 $'000
EQUITY				
Parent equity interest				
Contributed equity		1 008 014	998 034	915 296
Reserves		90 374	90 373	90 374
Accumulated deficit		(719 556)	(750 046)	(637 334)
TOTAL EQUITY		**378 832**	**338 361**	**368 336**

The above statement should be read in conjunction with the accompanying notes.

STATEMENT OF CHANGES IN EQUITY
for the period ended 30 June 2021

	2021 $'000	Original budget 2021 $'000	2020 $'000
RETAINED EARNINGS			
Opening balance	(637 334)	(637 334)	(570 080)
Adjustment on initial application of AASB16		-	22 823
Comprehensive income			
Deficit on continuing operations	(82 222)	(112 712)	(90 077)
Closing balance	***(719 556)***	***(750 046)***	**(637 334)**
ASSET REVALUATION RESERVE			
Opening balance	90 374	90 373	69 858
Other comprehensive income			
Changes in asset revaluation surplus	-	-	20 516
Closing balance	***90 374***	***90 373***	**90 374**
CONTRIBUTED EQUITY			
Opening balance	915 296	915 296	843 097
Transactions with owners			
Contributions by owners			
Equity injection—appropriation	10 456	10 456	10 870
Departmental capital budget	82 262	72 282	61 329
Closing balance	***1 008 014***	***998 034***	**915 296**
CLOSING BALANCE ATTRIBUTABLE TO THE AUSTRALIAN GOVERNMENT	**378 832**	**338 361**	**368 336**

The above statement should be read in conjunction with the accompanying notes.

Accounting policy

Equity injections

Amounts appropriated which are designated as 'equity injections' for a year (less any formal reductions) and Departmental Capital Budgets (DCBs) are recognised directly in contributed equity in that year.

STATEMENT OF CASH FLOWS
for the period ended 30 June 2021

	Notes	2021 $'000	Original budget 2021 $'000	2020 $'000
OPERATING ACTIVITIES				
Cash received				
Appropriations		452 579	484 639	473 967
Sales of services		12 440	22 215	18 452
Net GST received		17 581	24 042	23 884
Other		6453	1756	5533
Total cash received		***489 053***	***532 652***	***521 836***
Cash used				
Employees		274 926	279 926	273 653
Suppliers		154 541	153 942	183 282
Interest payments on lease liabilities		8029	9953	8414
Section 74		19 099	24 120	31 331
Other		-	192	-
Total cash used		***456 595***	***468 133***	***496 680***
NET CASH FROM/(USED BY) OPERATING ACTIVITIES		**32 458**	**64 519**	**25 156**
INVESTING ACTIVITIES				
Cash received				
Proceeds from property, plant, and equipment		417	-	641
Total cash received		***417***	***-***	***641***
Cash used				
Purchase of property, plant, equipment and computer software		83 946	102 334	79 404
Total cash used		***83 946***	***102 334***	***79 404***
NET CASH FROM/(USED BY) INVESTING ACTIVITIES		**(83 529)**	**(102 334)**	**(78 763)**

STATEMENT OF CASH FLOWS
for the period ended 30 June 2021 (continued)

	Notes	2021 $'000	Original budget 2021 $'000	2020 $'000
FINANCING ACTIVITIES				
Cash received				
Contributed equity		82 839	82 738	78 179
Total cash received		***82 839***	***82 738***	***78 179***
Cash used				
Principal repayments of lease liabilities		34 241	45 936	31 829
Total cash used		***34 241***	***45 936***	***31 829***
NET CASH FROM/(USED BY) FINANCING ACTIVITIES		**48 598**	**36 802**	**46 350**
Net increase (decrease) in cash held		(2473)	(1013)	(7257)
Cash and cash equivalents at the beginning of the reporting period		16 260	16 260	23 517
CASH AND CASH EQUIVALENTS AT THE END OF THE REPORTING PERIOD		**13 787**	**15 247**	**16 260**

The above statement should be read in conjunction with the accompanying notes.

NOTES TO AND FORMING PART OF THE FINANCIAL STATEMENTS

Overview

The basis of preparation

The financial statements are general purpose and required by section 42 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

The financial statements have been prepared in accordance with:

- Public Governance, Performance and Accountability (Financial Reporting) Rule 2015; and
- Australian Accounting Standards and Interpretations issued by the Australian Accounting Standards Board (AASB) that apply for the reporting period.

The financial statements have been prepared on an accrual basis and are in accordance with the historical cost convention, except for certain assets and liabilities at fair value. Except where stated, no allowance is made for the effect of changing prices on the results or the financial position. The financial statements are presented in Australian dollars.

ASIO has applied the exemption available under section 105D of the PGPA Act in preparing the financial statements. The effect of the application of this exemption is immaterial to the financial performance and position as disclosed in the financial statements.

New accounting standards

There were no new or revised accounting standards issued prior to the signing of the statement by the Director-General that are applicable to the current reporting period.

Taxation

ASIO is exempt from all forms of taxation except fringe benefits tax and the goods and services tax (GST).

Events after the reporting period

There was no subsequent event that had the potential to significantly affect the ongoing structure or financial position or performance of ASIO.

1. Financial performance

	2021 $'000	2020 $'000
1.1 EXPENSES		
1.1.A Employee benefits		
Wages and salaries	210 065	215 450
Superannuation	-	-
Defined contribution plans	23 049	22 709
Defined benefit plans	13 676	15 699
Leave and other entitlements	17 886	24 575
Separation and redundancies	586	8655
Total employee benefits	**265 262**	**287 088**
1.1.B Suppliers		
Goods supplied	10 148	6514
Services supplied	124 350	143 387
Operating lease rentals	1804	1320
Workers' compensation premiums	1139	778
Total supplier expenses	**137 441**	**151 999**

ASIO has no short-term lease commitments as at 30 June 2021.

The above lease disclosures should be read in conjunction with notes 1.1.C, 1.2.B, 2.2.A and 2.4.A.

Accounting policy

ASIO has elected not to recognise right-of-use assets and lease liabilities for short-term leases that have a lease term of 12 months or less and leases of low-value (less than $10 000). ASIO recognises the lease payments associated with these leases as an expense on a straight-line basis over the lease term.

1.1.C Finance costs		
Interest on lease liabilities	8029	8414
Unwinding of discount—restoration obligations	-	274
Total finance costs	**8029**	**8688**
1.1.D Write-down and impairment of other assets		
Write-down and impairment of property, plant, equipment and computer software	955	-
Losses from asset sales	361	425
Total write-down and impairment of other assets	**1316**	**425**

	2021 $'000	2020 $'000

1.2 OWN-SOURCE REVENUE AND GAINS

1.2.A Sale of services	**9266**	**18 019**

Accounting policy

Revenue from the sale of services is recognised by reference to the stage of completion of contracts at reporting date. This is determined by the proportion that costs incurred to date bear to the estimated total costs of the transaction.

1.2.B Other revenue

Subleased right-of-use assets income	**5126**	4305
Resources received free of charge—remuneration of auditors	**135**	135
Resources received free of charge—equipment	**428**	473
Other	**1327**	1228
Total other revenue	**7016**	**6141**

Subleased right-of-use assets income commitments

As lessor, subleased right-of-use assets income commitments are for office accommodation.

Commitments are receivable:

Within 1 year	**4075**	3929
Between 1 to 5 years	**17 835**	17 210
More than 5 years	**6373**	11 074
Total subleased right-of-use assets income commitments	***28 283***	***32 213***

Accounting policy

Resources received free of charge are recognised as revenue when, and only when, a fair value can be reliably determined and the services would have been purchased if they had not been donated. Use of those resources is recognised as an expense. Resources received free of charge are recorded as either revenue or gains depending on their nature.

2. Financial position

	2020 $'000	2019 $'000
2.1 FINANCIAL ASSETS		
2.1.A Trade and other receivables		
Goods and services	2289	3639
Appropriation receivable	133 615	102 018
GST receivable	5886	4372
Total trade and other receivables	**141 790**	**110 029**

All receivables are expected to be recovered in no more than 12 months.

Credit terms for goods and services were within 30 days (2020: 30 days).

Financial assets were assessed for impairment at 30 June 2021.
No indicators of impairment have been identified.

Accounting policy

Trade and other receivables are:

- held for the purpose of collecting contractual cash flows where the cash flows are solely payments of principal and interest and not provided at below-market interest rates;
- adjusted on initial measurement for expected credit losses; and
- subsequently measured at amortised cost using the effective interest method adjusted for any loss allowance.

2.2 NON-FINANCIAL ASSETS

2.2.A Reconciliation of property, plant, equipment and computer software

	Buildings	Buildings—leasehold improvement	Property, plant, equipment & computer software	Total
	$'000	$'000	$'000	$'000
As at 1 July 2020				
Gross book value	643 149	140 715	375 026	1 158 890
Accumulated depreciation, amortisation and impairment	(44 470)	(3 166)	(161 285)	(208 921)
Net book value 1 July 2020	***598 680***	***137 549***	***213 741***	***949 969***
Additions by purchase	986	826	75 110	76 922
Additions—internally developed	-	-	6089	6089
Depreciation and amortisation	(536)	(17 420)	(76 767)	(94 723)
Disposals	-	(76)	(702)	(778)
Right-of-use assets additions	2497	-	281	2778
Right-of-use assets depreciation	(44 331)	-	(2 968)	(47 299)
Net book value 30 June 2021	**557 296**	**120 879**	**214 783**	**892 958**
Gross book value	646 488	141 403	439 951	1 227 842
Accumulated depreciation, amortisation and impairment	(89 191)	(20 524)	(225 168)	(334 884)
Net book value 30 June 2021	**557 296**	**120 879**	**214 783**	**892 958**
Carrying amount of right-of-use assets	***549 793***	***-***	***11 443***	***561 236***

Impairment

Non-financial assets are assessed for impairment at the end of each reporting period. There are no indicators of impairment for property, plant, equipment and computer software. Any reduction in assets' carrying value due to impairment throughout the year has been accounted for in the statement of comprehensive income.

Sale or disposal

Property, plant, equipment and computer software of an immaterial value only is expected to be sold or disposed of within the next 12 months. No buildings are expected to be sold or disposed of within the next 12 months.

	Buildings	Buildings—leasehold improvement	Property, plant, equipment & computer software	Total
	$'000	$'000	$'000	$'000
Contractual commitments for the acquisition of property, plant, equipment and computer software				
Within 1 year	-	-	4206	4206
Between 1 to 5 years	-	-	1366	1366
Total capital commitments	**-**	**-**	***5572***	***5572***

Accounting policy

Acquisition of assets

The cost of acquisition includes the fair value of assets transferred in exchange and liabilities undertaken. Financial assets are initially measured at their fair value.

Purchases of non-financial assets are initially recognised at cost in the statement of financial position, except for purchases costing less than $4000 which are expensed in the year of acquisition (other than where they form part of a group of similar items which are significant in total).

Property, plant, equipment and computer software (excluding right-of-use assets)

Following initial recognition at cost, property, plant and equipment is carried at fair value less subsequent accumulated depreciation and accumulated impairment losses. Valuations are conducted with sufficient frequency to ensure that the carrying amounts of assets do not materially differ from the assets' fair values as at the reporting date. The regularity of independent valuations depends upon the volatility of movements in market values for the relevant assets.

Depreciable property, plant and equipment assets are written off to their estimated residual values over their estimated useful lives to ASIO using, in all cases, the straight-line method of depreciation. Leasehold improvements are depreciated on a straight-line basis over the lesser of the estimated useful life of the improvements or the unexpired period of the lease.

Depreciation rates (useful lives), residual values and methods are reviewed at each reporting date. Depreciation rates applying to each class of depreciable asset are based on the following useful lives.

	2021
Buildings on freehold land	**8–60 years**
Leasehold improvements	**lease term**
Plant and equipment	**2–25 years**

All assets were assessed for impairment at 30 June 2021. Where indications of impairment exist, the asset's recoverable amount is estimated and an impairment adjustment made if the asset's recoverable amount is less than its carrying amount.

An asset is derecognised upon disposal or when no further future economic benefits are expected from its use or disposal.

ASIO's computer software comprises purchased and internally developed software for internal use. These assets are carried at cost less accumulated amortisation and accumulated impairment losses.

Software is amortised on a straight-line basis over its anticipated useful life. The useful life of ASIO's software is 1–10 years (2020: 1–10 years).

Lease right-of-use assets

Lease right-of-use assets are capitalised at the commencement date of the lease and comprise the initial lease liability amount, initial direct costs incurred when entering into the lease less any lease incentives received. These assets are disclosed by Commonwealth lessees as separate asset classes, and presented with corresponding assets according to the nature of the lease.

Lease right-of-use assets are measured at cost after initial recognition and depreciated on a straight-line basis over the lease term.

Fair value measurement

ASIO's assets are held for operational purposes and not held for the purpose of deriving a profit. The current use of all non-financial assets is considered their highest and best use.

Comprehensive valuations are carried out at least once every three years. ASIO engaged the services of Jones Lang LaSalle (JLL) to conduct a review to assess whether materiality is evident between carrying amounts and fair value measurement for all non-financial assets (excluding software and lease right of use assets) as at 31 March 2021. JLL has provided written assurance to ASIO that the models developed are in compliance with *AASB 13 Fair Value Measurement*.

The methods utilised to determine and substantiate the unobservable inputs are derived and evaluated as follows:

Physical depreciation and obsolescence - Assets that do not transact with enough frequency or transparency to develop objective opinions of value from observable market evidence have been measured utilising the Current Replacement Cost approach. Under the Current Replacement Cost approach, the estimated cost to replace the asset is calculated and then adjusted to take into account physical depreciation and obsolescence. Physical depreciation and obsolescence has been determined based on professional judgement regarding physical, economic and external obsolescence factors relevant to the asset under consideration. For all leasehold improvement assets, the consumed economic benefit / asset obsolescence deduction is determined based on the term of the associated lease.

	2021 $'000	2020 $'000
2.3 PAYABLES		
2.3.A Suppliers		
Trade creditors and accruals	7526	9991
Total suppliers	**7526**	**9991**
Settlement is usually made within 30 days.		
2.3.B Other payables		
Salaries	4284	5415
Superannuation	673	554
Termination benefits	163	3794
Unearned income	1303	435
Fringe benefits tax	583	2222
Total other payables	**7006**	**12 420**
2.4 INTEREST BEARING LIABILITIES (LEASES)		
2.4.A Interest bearing liabilities (Leases)		
Lease liabilities—buildings	575 273	604 165
Lease liabilities—property, plant, equipment and computer software	11 792	14 367
Total interest bearing liabilities (Leases)	**587 064**	**618 532**
Total cash outflow for leases for the year ended 30 June 2021 was $42.270 million.		
Maturity analysis—contractual undiscounted cash flows		
Within 1 year	42 342	42 112
Between 1 to 5 years	128 752	168 145
More than 5 years	476 734	476 100
Total Leases	***647 828***	***686 357***

Accounting policy

For all new contracts entered into, ASIO considers whether the contract is, or contains a lease. A lease is defined as 'a contract, or part of a contract, that conveys the right to use an asset (the underlying asset) for a period of time in exchange for consideration'. Once it has been determined that a contract is, or contains, a lease, the lease liability is initially measured at the present value of the lease payments unpaid at the commencement date, discounted using the interest rate implicit in the lease, if that rate is readily determinable, or the Organisation's incremental borrowing rate. Subsequent to initial measurement, the liability will be reduced for payments made and increased for interest. It is remeasured to reflect any reassessment or modification to the lease. When the lease liability is remeasured, the corresponding adjustment is reflected in the right-of-use asset or profit and loss depending on the nature of the reassessment or modification.

	2021 $'000	2020 $'000
2.5 PROVISIONS		
2.5.A Employee provisions		
Leave	92 860	95 063
Termination benefits	170	1482
Total employee provisions	**93 030**	**96 545**

Accounting judgements and estimates

Leave provisions involve assumptions based on the expected tenure of existing staff, patterns of leave claims and payouts, future salary movements and future discount rates.

Accounting policy

Liabilities for 'short-term employee benefits' (as defined in *AASB 119 Employee Benefits*) and termination benefits expected within 12 months of the end of the reporting period are measured at nominal amounts.

The liability for employee entitlements includes provision for annual leave and long service leave. No provision has been made for sick leave, as all sick leave is non-vesting and the average sick leave taken in future years by employees of ASIO is estimated to be less than the annual entitlement for sick leave.

The leave liabilities are calculated on the basis of employees' remuneration at the estimated salary rates that will apply at the time the leave is taken, including ASIO's employer superannuation contribution rates, to the extent that the leave is likely to be taken during service rather than paid out on termination.

The liability for leave has been determined by reference to the work of an actuary as at May 2020. An assessment of ASIO's staff profile at balance date was performed; the assessment determined that the data profile used by the actuary is still relevant at balance date. The estimate of present value of the liability takes into account attrition rates and pay increases through promotion and inflation.

Staff of ASIO are members of the Commonwealth Superannuation Scheme (CSS), the Public Sector Superannuation Scheme (PSS), the PSS accumulation plan (PSSap) or other complying superannuation funds.

The CSS and PSS are defined benefit schemes for the Australian Government. The PSSap and other complying funds are defined contribution schemes.

The liability for defined benefits is recognised in the financial statements of the Australian Government and is settled by the Australian Government in due course. This liability is reported in the Department of Finance's administered schedules and notes.

ASIO makes employer contributions to employees' superannuation schemes at rates determined by an actuary to be sufficient to meet the current cost to the Government. ASIO accounts for the contributions as if they were contributions to defined contribution plans.

Superannuation payable as at 30 June represents outstanding contributions for the final fortnight of the year.

	2021 $'000	2020 $'000
2.5.B Restoration obligations	**8273**	**7225**
Carrying amount 1 July	7225	6794
Additional provisions made	1104	157
Reduction in value	-	-
Unwinding of discount or change in discount rate	(56)	274
Closing balance	***8273***	***7225***

ASIO has a number of agreements for the leasing of premises, which contain provisions requiring restoration of the premises to original condition at the conclusion of the lease. ASIO has made a provision to reflect the present value of this obligation.

3. Funding

3.1 APPROPRIATIONS

3.1.A Annual departmental appropriations

	Ordinary annual services	Capital budget[1]	Equity injections
	$'000	$'000	$'000
2021			
Appropriation Act			
Annual appropriation[2]	455 198	82 262	10 456
PGPA Act			
Section 74 transfers	19 099	-	-
Total appropriation	**474 297**	**82 262**	**10 456**
Appropriation applied (current and prior years)	(454 432)	(72 782)	(10 057)
Variance	***19 865***	***9480***	***399***

[1] Departmental Capital Budgets are appropriated through Supply Acts (No. 1) and Appropriation Acts (No. 1,3). They form part of ordinary annual services, and are not separately identified in the Supply/Appropriation Acts.

[2] $9.980 million was permanently withheld in accordance with PGPA Act section 51.

Ordinary annual appropriation remains unspent in 2021 due to reduced supplier purchases resulting from COVID-19 restrictions.

Capital appropriations remain unspent due to the timing of asset purchases.

The Department of Foreign Affairs and Trade spends money from the Consolidated Revenue Fund on behalf of ASIO in relation to services overseas: $5.631 million (2020: $7.583 million).

2020			
Appropriation Act			
Annual appropriation	473 011	61 329	10 870
PGPA Act			
Section 74 transfers	31 331	-	-
Total appropriation	**504 342**	**61 329**	**10 870**
Appropriation applied (current and prior years)	(472 670)	(69 829)	(8 350)
Variance	***31 672***	***(8500)***	***2520***

The 2020 operating appropriation was unspent in 2020 due to the timing of supplier purchases.

Variances in 2020 Capital appropriations are due to prior year appropriations applied in the current year.

	2021	2020
	$'000	$'000
3.1.B Unspent departmental annual appropriations (recoverable GST exclusive)		
Appropriation Act (No. 1) 2019–20	-	92 888
Appropriation Act (No. 2) 2019–20	-	5481
Appropriation Act (No. 3) 2019–20	-	17 870
Appropriation Act (No. 4) 2019–20	-	2039
Appropriation Act (No. 1) 2020–21[3]	139 483	-
Supply Act (No. 2) 2020–21	3000	-
Appropriation Act (No. 2) 2020–21	4919	-
Appropriation Act (No. 3) 2020–21	9980	-
Total	**157 382**	**118 278**

[3] This balance includes $9.980m that has been permanently withheld by the Department of Finance and as such the Organisation is unable to utilise the amount for departmental purposes.

3.1.C Net cash appropriation arrangements

Total surplus (deficit) excluding depreciation, amortisation and lease principal repayments	**25 559**	**17 106**
Depreciation and amortisation (excluding right-of-use leased assets)	(94 724)	(92 283)
Depreciation—right-of-use leased assets	(47 298)	(46 826)
Principal repayments—leases	34 241	31 926
Deficit as per statement of comprehensive income	(82 222)	(90 077)

From 2010-11, the government introduced net cash appropriation arrangements where revenue appropriations for depreciation / amortisation expenses ceased. Entities now receive a separate capital budget provided through equity appropriations. Capital budgets are to be appropriated in the period when cash payment for capital expenditure is required.

The inclusion of depreciation/amortisation expenses related to right-of-use leased assets and the lease liability principal repayment amount reflects the cash impact on implementation of *AASB 16 Leases*. It does not directly reflect a change in appropriation arrangements.

4. Managing uncertainties

	2021	2020
	$'000	$'000

4.1 CONTINGENT ASSETS AND LIABILITIES

Quantifiable contingencies

ASIO's contingent liabilities relate to claims for damages or costs. The amount represents an estimate of ASIO's liability based on precedent in such cases. ASIO is defending the claims.

Contingent liabilities

Balance from previous period	200	-
New contingent liabilities recognised	600	200
Liabilities realised	(200)	-
Total contingent liabilities	**600**	**200**

Unquantifiable contingencies

At 30 June 2021, ASIO had a number of legal claims against it. ASIO has denied liability and is defending the claims. It is not possible to estimate the amounts of any eventual payments that may be required in relation to these claims.

Accounting policy

Contingent liabilities and contingent assets are not recognised in the statement of financial position but are reported in the relevant schedules and notes. They may arise from uncertainty as to the existence of a liability or asset, or represent an existing liability or asset in respect of which the amount cannot be reliably measured. Contingent assets are reported when settlement is probable, but not virtually certain, and contingent liabilities are recognised when settlement is greater than remote.

4.2 FINANCIAL INSTRUMENTS

4.2.A Categories of financial instruments

Financial assets at amortised cost

Cash	13 787	16 260
Trade receivables	2289	3639
Accrued revenue	493	602
Total financial assets	**16 569**	**20 501**

Financial liabilities at amortised cost

Trade creditors and accruals	7526	9991
Total financial liabilities	**7526**	**9991**

The net fair values of the financial assets and liabilities are at their carrying amounts. ASIO derived no interest income from financial assets for the period ending 30 June 2021 (2020: nil).

There was no net gain or loss from financial assets or liabilities through profit or loss for the period ending 30 June 2021 (2020: nil).

Accounting policy

Financial assets

ASIO classifies its financial assets as 'measured at amortised cost'. Financial assets included in this category must meet two criteria:

- the financial asset is held in order to collect the contractual cash flows; and
- the cash flows are solely payments of principal and interest on the principal outstanding amount.

Amortised cost is determined using the effective interest method with income recognised on an effective interest rate basis.

Financial assets are recognised when ASIO becomes party to a contract and, as a consequence, has a legal right to receive or obligation to pay cash and derecognised when the contractual rights to the cash flows from the financial asset expire or are transferred upon trade date.

Financial assets are assessed for impairment at the end of each reporting period. Allowances are made when collectability of the debt is no longer probable.

Financial assets are assessed for impairment at the end of each reporting period based on an amount equal to the lifetime expected credit losses. A write-off directly reduces the gross carrying amount of the financial asset.

Financial liabilities

Supplier and other payables are recognised at amortised cost. Liabilities are recognised to the extent that the goods or services have been received (and irrespective of having been invoiced). Supplier and other payables are derecognised on payment.

5. Other information

	2021 $'000	2020 $'000
5.1 CURRENT/NON-CURRENT DISTINCTION FOR ASSETS AND LIABILITIES		
Assets expected to be recovered in:		
No more than 12 months		
Cash and cash equivalents	13 787	16 260
Trade and other receivables	141 790	110 029
Accrued revenue	493	602
Amortisation of subleased right-of-use assets income	(100)	(238)
Prepayments	25 707	24 663
Total no more than 12 months	***181 677***	***151 316***
More than 12 months		
Amortisation of subleased right-of-use assets income	1779	1679
Prepayments	5450	10 085
Land and buildings	678 175	736 228
Property, plant, equipment and computer software	214 783	213 740
Total more than 12 months	***900 187***	***961 733***
Total assets	**1 081 864**	**1 113 049**
Liabilities expected to be recovered in:		
No more than 12 months		
Suppliers	7526	9991
Other payables	7006	12 420
Leases	1560	375
Employee provisions	23 256	24 674
Restoration obligations	2146	239
Other provisions	132	-
Total no more than 12 months	***41 626***	***47 699***
More than 12 months		
Leases	585 505	618 157
Employee provisions	69 774	71 871
Restoration obligations	6127	6986
Total more than 12 months	***661 406***	***697 014***
Total liabilities	**703 032**	**744 713**

5.2 KEY MANAGEMENT PERSONNEL REMUNERATION

Key management personnel are those persons having authority and responsibility for planning, directing and controlling the activities of ASIO, directly or indirectly. ASIO has determined key management personnel to be the Director-General and members of the Executive Committee.

	2021	2020
	$'000	$'000
Short-term employee benefits	**2047**	2183
Long-term employee benefits	**144**	68
Termination benefits	**-**	301
Post-employment benefits	**343**	339
Total key management personnel remuneration expenses[4]	**2534**	**2891**

The number of key management positions as at 30 June 2021 is 5 (2020: 6).

Membership of the Executive Committee changed throughout 2019–20. Several key management positions were occupied by different officers for portions of the year, which was not the case in 2020–21.

[4] The above key management personnel remuneration excludes the remuneration and other benefits of the portfolio ministers whose remuneration and other benefits are set by the Remuneration Tribunal and are not paid by ASIO.

5.3 RELATED PARTY DISCLOSURES

Related party relationships

ASIO is an Australian Government–controlled entity. ASIO's related parties are key management personnel including the portfolio ministers and Executive Committee, and other Australian Government entities.

Transactions with key management personnel

Given the breadth of government activities, key management personnel and their associates may transact with the government sector in the same capacity as ordinary citizens. Such transactions include the payment or refund of taxes, receipt of a Medicare rebate or higher education loans. These transactions are not disclosed in this note.

All related party transactions with key management personnel during 2020–21 were in the ordinary course of business and do not require separate disclosure.

Transactions with other Australian Government entities

ASIO transacts with Commonwealth Government entities at arm's length for the provision of goods and services in the normal course of business. These transactions are not disclosed in this note.

ASIO has a significant relationship with the Department of Finance as lessor of the organisation's headquarters in Canberra. Lease payments were $24.136 million in 2020–21.

5.4 MAJOR BUDGET VARIANCES

The following provides an explanation of variances between the original budget as presented in the 2020–21 Portfolio Budget Statements (PBS) and the 2020–21 final actual result. The budget is not audited. Explanations are provided for major budget variances only. Variances are treated as major when they are considered important for the reader's understanding or are relevant to an assessment of the discharge of accountability and to an analysis of ASIO's performance.

The nature and timing of the Commonwealth's budget process can also contribute to the variances. The original budget as presented in the 2020–21 PBS is amended by Government throughout the year. ASIO's budget for 2020–21 was updated as part of the 2020–21 Mid-Year Economic Fiscal Outlook (MYEFO).

The impact of COVID-19 and the disruption to economic activity during 2020–21 was estimated and factored into budget estimates; however, the actual ongoing impact was not fully anticipated in the budget figures. The continuing travel restrictions disrupted travel by the Organisation and impacted the supply of goods and services, contributing to underspends in some expense categories.

Expenses

The total variance between actual expenses and the original budget is a decrease of $48.084 million (8%) including the following.

- Depreciation and amortisation expenses were $16.625 million lower than original budget due to delays in the timing of asset purchases and the inflated estimate of the initial application of AASB 16 Leases included in the budget estimates (refer to 'Liabilities' below).
- Employee benefits were $15.650 million lower than original budget due to lower than anticipated staffing levels and an increase in the discount rate used to calculate employee provisions.
- Supplier expenses were $15.201 million lower than original budget as the impact of COVID-19 on suppliers led to delays and deferral of supply and the Organisation's reduced ability to continue planned activity given the adjustments required to operate under COVID-19 restrictions.

Income

Income is $17.595 million (3%) lower than original budget. The decrease is due to including the following.

- A decrease of $9.980 million in appropriation funding as a result of funds being permanently withheld in accordance with PGPA Act section 51 and re-appropriated as capital funding at 2020–21 Additional Estimates (refer to 'Statement of changes in equity' below).
- An increase in other revenue of $4.369 million relating to rental income which was unknown at the time of budget preparation.
- Own source revenue was $7.615 million less than budget. This budget is dependent on the number of requests and activities undertaken by external parties which was less than anticipated as a result of COVID-19 restrictions.

Assets

Total assets are $20.391 million lower (5%) than original budget. Financial assets are $51.106 million higher than budget. The largest variance is within appropriation receivable which includes undrawn appropriation as a result of reduced expenditure through the year. These funds form part of the receivables balance and will be available in 2021–22.

Non-financial assets are $71.497 million lower than original budget. This variance is a result of the 2020–21 Budget Estimate, including an inflated estimate of the initial application of AASB 16 Leases (refer to 'Liabilities' below) combined with asset purchases being less than anticipated.

Liabilities

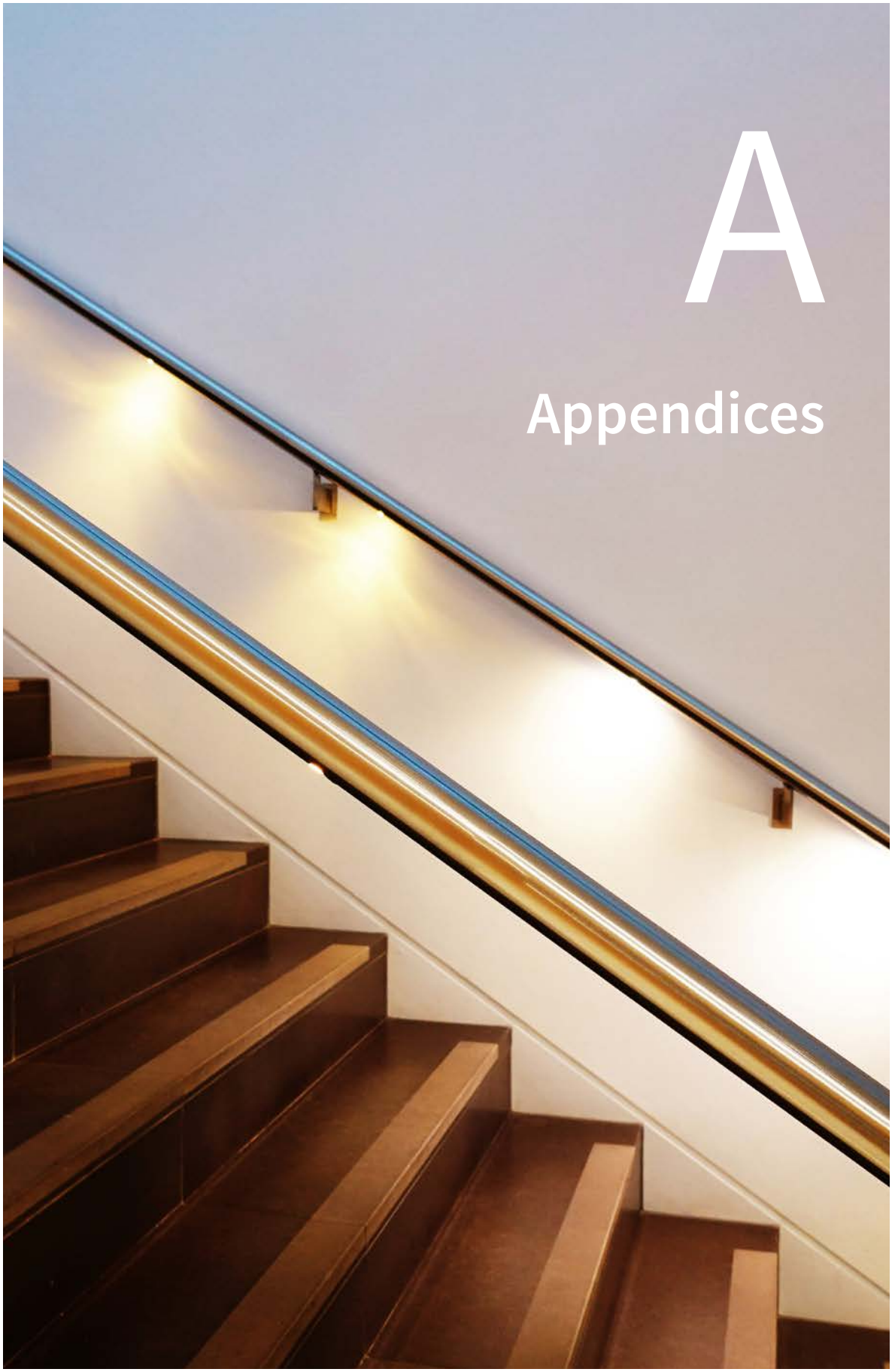
Total liabilities are $60.862 million lower (8%) than original budget. The variance is attributable to lease liabilities ($51.419 million). During 2020–21, errors in the estimated application of AASB 16 Leases were identified in the 2020–21 Budget Estimate, which resulted in the recognition of an inflated number of new leases over the budgeted forward estimates.

Statement of changes in equity

Total equity is $40.471 million higher (12%) than budget. The result is primarily attributable to a surplus excluding depreciation, amortisation and lease principal repayments compared to a budgeted breakeven result. The remaining increase relates to the re-appropriation of quarantined ordinary annual appropriation (in accordance with PGPA Act section 51) to capital appropriation at 2020–21 Additional Estimates.

Statement of cash flows

The amounts reported in the statement of cash flows are interrelated with figures disclosed in the statement of comprehensive income and statement of financial position. Consequently, cash flow variances are attributable to the relevant variance explanations provided above.



A

Appendices

Appendix A: ASIO resource statement

	Actual available appropriation 2021 $'000	Payments made 2021 $'000	Balance remaining 2021 $'000
Departmental			
Annual appropriations—ordinary annual services[1]			
Prior year appropriation	94 498	94 498	-
Departmental appropriation[2]	455 198	355 554	99 644
Section 74 external revenue[3]	18 479	13 406	5072
Departmental capital budget[4]	82 262	61 282	20 980
Cash on hand	16 260	2473	13 787
Annual appropriations—other services—non-operating[5]			
Prior year appropriation	7520	7520	-
Equity injections	10 456	2537	7919
Total net resourcing and payments for ASIO	**684 673**	**537 270**	**147 402**

[1] Supply Act (No.1), Appropriation Act (No.1) and Appropriation Act (No.3)

[2] Excludes departmental capital budget (DCB) and $9.980 million which was permanently withheld in accordance with PGPA Act section 51

[3] External receipts under section 74 of the *Public Governance, Performance and Accountability Act 2013*

[4] Departmental capital budgets are not separately identified in Supply Act (No.1), Appropriation Act (No.1) and Appropriation Act (No.3) and form part of ordinary annual services items. For accounting purposes, this amount has been designated as a 'contribution by owner'.

[5] Supply Act (No.2), Appropriation Act (No.2)

Appendix B: expenses by outcomes

Outcome 1: To protect Australia, its people and its interests from threats to security through intelligence collection, assessment and advice to Government	Budget* 2021 $'000	Actual expenses 2021 $'000	Variation 2021 $'000
Program 1.1: Security Intelligence			
Departmental expenses			
Departmental appropriation	455 198	427 247	27 951
Section 74 external revenue[1]	24 120	18 479	5641
Expenses not requiring appropriation in the budget year[2]	112 857	108 345	4512
Total for Program 1.1	***592 175***	***554 072***	***38 103***
Total expenses for Outcome 1	**592 175**	**554 072**	**38 103**

* Full-year budget, including any subsequent adjustments made at Additional Estimates and reductions under *Public Governance, Performance and Accountability Act 2013* section 51

[1] Expenses incurred in relation to receipts retained under *Public Governance, Performance and Accountability Act 2013* section 74

[2] Expenses not requiring appropriation in the budget year are depreciation, amortisation expenses and resources received free of charge

Appendix C: executive remuneration

Key management personnel remuneration

Categories of ASIO's key management personnel include:

- the Director-General of Security;
- members of the Executive Committee;
- Senior Executive Service (SES) employees; and
- other highly paid staff.

Remuneration policies, practices and governance

The Director-General's remuneration is set by the Remuneration Tribunal under section 13 of the *Remuneration Tribunal Act 1973*.

Remuneration of ASIO's senior executive employees is established through determinations made under section 84 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), and guided by the Australian Government's Workplace Bargaining Policy 2018.

There were no general increases to SES remuneration during the 2020–21 reporting period.

The following tables show the remuneration for key management personnel, senior executives and other highly paid staff in 2020–21 in accordance with the Public Governance, Performance and Accountability Rule.

Information about remuneration for key management personnel

		Short-term benefits			Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration
Name	Position title	Base salary[1] $	Bonuses $	Other benefits and allowances $	Superannuation contributions $	Long service leave[2] $	Other long-term benefits $	$	$
Mike BURGESS	Director-General	594 048	0	0	89 409	12 568	0	0	696 026
Heather COOK	Deputy Director-General	364 735	0	0	66 879	-6 627	0	0	424 988
Hazel BENNETT	Deputy Director-General	444 050	0	0	79 095	62 522	0	0	585 666
Name withheld[3]	Strategic Advisor	325 590	0	0	56 630	6 118	0	0	388 337
Name withheld[4]	General Counsel	318 160	0	0	51 136	69 321	0	0	438 617

[1] This includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements as per the *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*.

[2] This does not represent one year's leave accrual at officer's current salary. The value is in accordance with Department of Finance requirements as per the *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*. Discount rate variations throughout the year will affect the value.

[3] The Strategic Advisor is a non-declared officer. To comply with section 92 of the ASIO Act and the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the Strategic Advisor's name has not been provided in the annual report.

[4] The General Counsel is a non-declared officer. To comply with section 92 of the ASIO Act and the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the General Counsel's name has not been provided in the annual report.

Information about remuneration for senior executives

		Short-term benefits			Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration
Total Remuneration bands	Number of senior executives	Average base salary[1] $	Average bonuses $	Average other benefits and allowances $	Average superannuation contributions $	Average long service leave[2] $	Average other long-term benefits $	Average termination benefits $	Average total remuneration $
$0 to $230 000	27	55 418	0	493	9 188	1 336	0	5 642	72 077
$230 001 to $255 000	8	177 945	0	1 320	33 712	-1 309	0	31 738	243 406
$255 001 to $280 000	19	225 955	0	2 464	42 294	-926	0	0	269 786
$280 001 to $305 000	5	249 702	0	3 346	42 262	-318	0	0	294 992
$305 001 to $330 000	5	252 932	0	9 494	46 341	7 961	0	0	316 727
$330 001 to $355 000	2	298 364	0	2 324	43 175	4 704	0	0	348 566
$355 001 to $380 000	1	316 387	0	0	47 073	5 609	0	0	369 070
$405 001 to $430 000	2	318 280	0	0	45 024	54 818	0	0	418 122
$430 001 to $455 000	3	359 303	0	9 853	49 813	20 697	0	0	439 667

[1] This includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements as per the *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*.

[2] This does not represent one year's leave accrual at officer's current salary. The value is in accordance with Department of Finance requirements as per the *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*. Discount rate variations throughout the year will affect the value.

Information about remuneration for other highly paid staff

		Short-term benfits			Post-employment benefits	Other long-term benefits		Termination benefits	Total remuneration
Remuneration band	Number of highly paid staff	Average base salary[1] $	Average bonuses $	Average other benefits and allowances $	Average superannuation contributions $	Average long service leave[2] $	Average other long-term benefits $	Average termination benefits $	Average total remuneration $
$230 001 to $255 000	16	188 901	0	9 202	27 912	3 735	0	10 185	239 935
$255 001 to $280 000	8	222 285	0	8 466	26 443	8 947	0	0	266 142
$280 001 to $305 000	4	171 994	0	39 771	18 688	59 211	0	0	289 663
$305 001 to $330 000	2	260 837	0	18 666	25 594	4 866	0	0	309 963
$330 001 to $355 000	1	305 220	0	10 579	27 465	5 026	0	0	348 289
$405 001 to $430 000	1	356 798	0	15 351	29 987	2 994	0	0	405 130

[1] This includes base salary, salary-related allowances and annual leave calculated in accordance with Department of Finance requirements as per the *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*.

[2] This does not represent one year's leave accrual at officer's current salary. The value is in accordance with Department of Finance requirements as per the *Resource management guide no. 138: Commonwealth entities executive remuneration reporting guide for annual reports*. Discount rate variations throughout the year will affect the value.

Appendix D: ASIO's salary classification structure

Employment salary ranges by classification level (minimum/maximum)—current reporting period (2020–21)

Senior Executive Service	Minimum salary	Maximum salary
SES Band 3	$327 377	$393 240
SES Band 2	$254 717	$279 500
SES Band 1	$203 774	$227 697
Senior employees		
AEE3		$163 131
AEE2	$137 858	$163 131
AEE1	$120 282	$134 407
Employees		
AE6	$94 632	$106 629
AE5	$85 624	$91 913
AE4	$78 024	$83 721
AE3	$69 004	$75 401
AE2	$60 695	$67 220
AE1	$52 385	$58 190
Salary range		
Minimum/maximum range	$52 385	$393 240

Note: Figures are at 30 June 2021. The salary figures include a 7.5 per cent service allowance. The service allowance is paid to all employees and recognises the imposition of security, professional and personal restrictions applicable to working at ASIO.

Appendix E: workforce statistics by headcount

Public Governance, Performance and Accountability Rule (PGPA Rule) section 17AG(4)(b)(i)–(iv)

Classification and gender of ongoing employees—current reporting period (2020–21)

	Male			Female			Indeterminate			
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total indeterminate**	**Total**
SES 3	1	0	1	2	0	2	0	0	0	3
SES 2	4	0	4	6	0	6	0	0	0	10
SES 1	21	0	21	16	0	16	0	0	0	37
AEE1–3	366	17	383	185	69	254	0	0	0	637
AE1–6	572	23	595	477	162	639	0	0	0	1234
Total	***964***	***40***	***1004***	***686***	***231***	***917***	***0***	***0***	***0***	***1921***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

PGPA Rule section 17AG(4)(b)(i)–(iv)

Classification and gender of non-ongoing employees—current reporting period (2020–21)

	Male			Female			Indeterminate			
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total indeterminate**	**Total**
SES 3	0	0	0	0	0	0	0	0	0	0
SES 2	0	0	0	0	0	0	0	0	0	0
SES 1	0	0	0	0	0	0	0	0	0	0
AEE1–3	0	3	3	0	1	1	0	0	0	4
AE1–6	3	7	10	2	3	5	0	0	0	15
Total	***3***	***10***	***13***	***2***	***4***	***6***	***0***	***0***	***0***	***19***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

PGPA Rule section 17AG(4)(b)(i)–(iv)

Classification and gender of ongoing employees—previous reporting period (2019–20)

	Male			Female			Indeterminate			
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total indeterminate**	**Total**
SES 3	1	0	1	2	0	2	0	0	0	3
SES 2	10	0	10	5	0	5	0	0	0	15
SES 1	24	0	24	20	0	20	0	0	0	44
AEE1–3	367	23	390	190	76	266	0	0	0	656
AE1–6	590	20	610	487	165	652	0	0	0	1262
Total	***992***	***43***	***1035***	***704***	***241***	***945***	***0***	***0***	***0***	***1980***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

PGPA Rule section 17AG(4)(b)(i)–(iv)

Classification and gender of non-ongoing employees—previous reporting period (2019–20)

	Male			Female			Indeterminate			
	Full-time	Part-time	**Total male**	Full-time	Part-time	**Total female**	Full-time	Part-time	**Total indeterminate**	**Total**
SES 3	0	0	0	0	0	0	0	0	0	0
SES 2	0	0	0	0	0	0	0	0	0	0
SES 1	0	0	0	0	0	0	0	0	0	0
AEE1–3	2	5	7	0	1	1	0	0	0	8
AE1–6	5	6	11	1	4	5	0	0	0	16
Total	***7***	***11***	***18***	***1***	***5***	***6***	***0***	***0***	***0***	***24***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

PGPA Rule section 17AG(4)(b)(i)–(iii)

Employees by full-time and part-time employment status—current reporting period (2020–21)

	Ongoing			Non-ongoing			
	Full-time	Part-time	**Total ongoing**	Full-time	Part-time	**Total non-ongoing**	**Total**
SES 3	3	0	3	0	0	0	0
SES 2	10	0	10	0	0	0	0
SES 1	37	0	37	0	0	0	0
AEE1–3	551	86	637	0	4	4	8
AE1–6	1049	185	1234	5	10	15	16
Total	***1650***	***271***	***1921***	***5***	***14***	***19***	***24***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

PGPA Rule section 17AG(4)(b)(i)–(iii)

Employees by full-time and part-time employment status—previous reporting period (2019–20)

	Ongoing			Non-ongoing			
	Full-time	Part-time	**Total ongoing**	Full-time	Part-time	**Total non-ongoing**	**Total**
SES 3	3	0	3	0	0	0	0
SES 2	15	0	15	0	0	0	0
SES 1	44	0	44	0	0	0	0
AEE1–3	557	99	656	2	6	8	8
AE1–6	1077	185	1262	6	10	16	16
Total	***1696***	***284***	***1980***	***8***	***16***	***24***	***24***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, ASIO employee (AE) and ASIO executive employee (AEE) numbers have been consolidated into classification categories.

PGPA Rule section 17AG(4)(b)(v)

Employment type by location—current reporting period (2020–21)

	Ongoing	Non-ongoing	Total
All locations	1921	19	1940
Total	***1921***	***19***	***1940***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the location of ASIO employees is classified and has been reported collectively in the 'All locations' category.

PGPA Rule section 17AG(4)(b)(v)

Employment type by location—previous reporting period (2019–20)

	Ongoing	Non-ongoing	Total
All locations	1980	24	2004
Total	***1980***	***24***	***2004***

Note: To avoid prejudice to ASIO's activities and to comply with the determination issued to ASIO under section 105D of the *Public Governance Performance and Accountability Act 2013*, the location of ASIO employees is classified and has been reported collectively in the 'All locations' category.

PGPA Rule section 17AG(4)(b)(vi)

Indigenous employment—current reporting period (2020–21)

	Total
Ongoing	8
Non-ongoing	0
Total	***8***

PGPA Rule section 17AG(4)(b)(vi)

Indigenous employment—previous reporting period (2019–20)

	Total
Ongoing	9
Non-ongoing	0
Total	***9***

PGPA Rule section 17AH(1)(c)

People with disability employment—current reporting period (2020–21)

	Total
Ongoing	27
Non-ongoing	0
Total	***27***

PGPA Rule section 17AH(1)(c)

People with a disability employment—previous reporting period (2019–20)

	Total
Ongoing	23
Non-ongoing	0
Total	***23***

Appendix F: work health and safety

Work health and safety considerations are integrated into the planning and delivery of ASIO's activities across a range of work environments.

Our focus is on identifying and monitoring safety risks, implementing appropriate controls and promoting a strong safety culture.

Safety risk management strategies reinforce legislative compliance and a culture of continual improvement. ASIO has a range of initiatives to educate and build workplace safety awareness within the workforce and to promote wellbeing.

COVID-19

The ongoing complexities associated with the COVID-19 pandemic continue to challenge ASIO and the safety of its workforce. The Organisation actively engages with these safety risks, adopting innovative, practical solutions to optimise our ability to undertake our activities safely. A number of ASIO's staff were vaccinated as part of Australia's COVID-19 vaccine roll-out strategy, with the balance of the workforce encouraged to receive a vaccination as soon as they are able to.

Health and wellbeing

ASIO continues to provide a range of health and wellbeing initiatives to its workforce to promote positive physical and psychological health. Our corporate program encourages staff to take proactive steps for their wellbeing and supports them to:

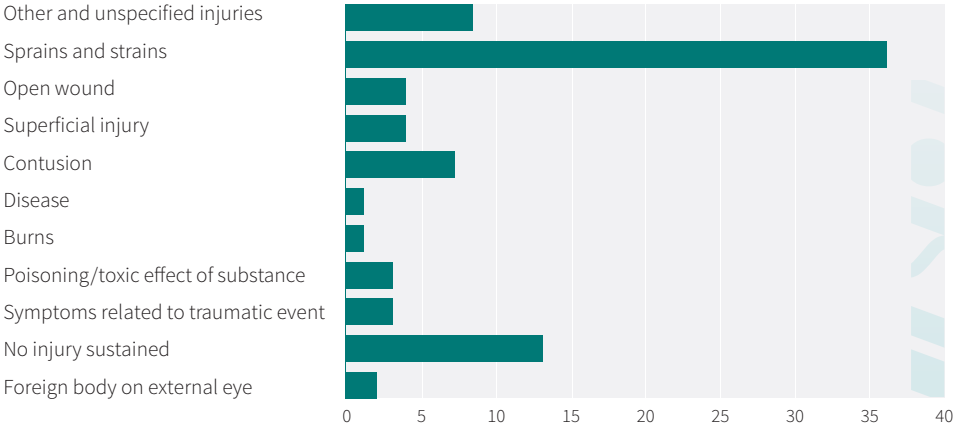
- participate in the workplace influenza vaccination program;
- engage with ASIO's support services, such as the Employee Assistance Program and Manager Assist service, when required;
- build an awareness of current and emerging health, safety and wellbeing issues; and
- develop a strong safety culture within their team.

Incidents

In accordance with legislated notification obligations, ASIO reported three incidents to Comcare in 2020–21.

Comcare initiated an investigation into one incident and subsequently issued ASIO with an improvement notice under section 191 of the *Work, Health and Safety Act 2011*. The notice, issued on 30 October 2020, identified a number of breaches to the work health and safety regulations. Remedial action was undertaken and Comcare confirmed closure of the notice on 22 December 2020, noting that all required actions had been completed.

Table 5: Total number of injuries by type



Appendix G: recruitment, advertising and market research

ASIO is committed to attracting the best and brightest people. We seek to reflect the diversity of the community we protect, and continue to develop and implement attraction strategies to achieve this.

In the financial year 2020–21, ASIO expended $314 183 on advertising and marketing for recruitment activities and campaigns.

Further information on these advertising campaigns is available at www.asio.gov.au and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website.

During the reporting year, ASIO continued to adapt and refine its approach to online recruitment due to the evolving COVID environment.

While non-intelligence roles remain an integral part of ASIO, during 2020–21 there was a greater focus on growing our own capability through entry-level technology and intelligence fields which will improve our capacity to operate in a more complex threat environment. ASIO also advertised its first Affirmative Measures round to attract Indigenous candidates to corporate security vetting roles.

ASIO continues to increase its reach to the community through its presence on social media platforms such as Twitter.

Appendix H: ecologically sustainable development and environmental performance

ASIO is committed to enhancing its environmental sustainability. We strive to operate in an environmentally responsible manner, making every effort to use our resources efficiently and manage our waste effectively.

Theme	Performance measure	Indicator(s)	2019–20	2020–21
Energy efficiency	Total consumption of building energy	Amount of electricity consumed (kWh)	24 779 371	24 980 635
		Amount of gas consumed (MJ)	13 094 381	14 149 220
		Amount of other fuels (diesel) consumed (L)	89 518	101 197
	Total production of energy from sources other than grid-connected electricity provider	Total amount of energy produced (kWh) from alternative sources	377 471	443 834
		Energy produced (kWh) from gas cogeneration plant	121 500	180 072
		Energy produced (kWh) from solar panels (green energy)	255 971	263 762
	Greenhouse gas emissions	Amount of greenhouse gases produced (tonnes)	26 417	23 886
	Environmental performance targets—tenant light & power (TL&P) and central services	TL&P less than 7500 MJ/person/annum	12 046	11 956
		Central services less than 400 MJ/m^2/annum	498	575
	Energy rating	NABERS[1] energy for offices (1–6)	3.5 stars	3.5 stars

[1] The National Australian Built Environment Rating System (NABERS) measures a building's energy efficiency, carbon emissions, water consumption, and waste produced and delivers a performance based on a rating from 1 to 6, expressed as a number of stars for comparison with similar buildings.

Theme	Performance measure	Indicator(s)	2019–20	2020–21
	Steps taken to reduce effect	**Measures to review and improve reducing the effect**		
	Implementation of a program of LED light replacement to reduce fluorescents	Increased use of video web-conferencing systems to offset carbon emission previously generated by inter-office travel		
		Participation in national environmental events such as Earth Hour		
Waste	Total waste production—this includes all waste (unwanted by products) produced when undertaking the functions of the agency	Amount of waste produced (tonnes)	197.3	194.98
	Un-recyclable waste production—this includes all wastes that are not re-used or recycled	Amount of waste going to landfill (tonnes)	77.1	57.59
	Recyclable waste production (excluding office paper)	Amount of waste going to recycling facilities (tonnes)	120.2	137.39
	Paper usage	Amount of waste paper going to recycling facilities (tonnes)	10.9	8.40
		Amount of paper sourced from recyclable sources (tonnes)	2.2	1.30
		Percentage of paper sourced from recyclable sources (%)	20	20
	Relative waste production	Amount of the total waste (kg) per employee	89.5	87.05
	Waste rating	NABERS waste rating (1–6)	3 stars	3 stars

Theme	Performance measure	Indicator(s)	2019–20	2020–21
	Steps taken to reduce effect	**Measures to review and improve reducing the effect**		
	'Follow-me' printing and double-sided printing and copying as the default setting on printers to reduce waste and paper expenses Sourced office copy paper from sustainably managed sources Used polystyrene recycling and e-waste management initiatives	Developed a waste-management strategy to align with NABERS waste assessment Built a culture of environmental awareness across our Organisation through sustainable initiatives based on the following principles: ■ reduce ■ re-use ■ recycle ■ recover ■ disposal.		
Water	Total consumption of water—this includes all water consumed when undertaking agency functions	Amount of water consumed (kL)	54 240	48 245
	Rainwater capture and use—includes all rainwater captured on site	Amount of rainwater captured (kL)	13.5	15.33
		Amount of captured rainwater used (kL)	13.5	15.33
	Relative consumption of water—per employee	Amount of total water used (kL) per employee	32.5	30.26
	Water rating	NABERS water rating (1–6)	1.5 stars	1.5 stars
	Steps taken to reduce effect	**Measures to review and improve reducing the effect**		
	ASIO uses fresh water from the public water network, artesian water sources and rainfall	Captured stormwater for irrigation and toilet flushing, reducing reliance on potable and bore water		

[1] The National Australian Built Environment Rating System (NABERS) measures a building's energy efficiency, carbon emissions, water consumption, and waste produced—and delivers a performance based on a rating from 1 to 6, expressed as a number of stars, for comparison with similar buildings.

Appendix I: report of the Independent Reviewer of Adverse Security Assessments

The Independent Reviewer of Adverse Security Assessments, Robert Cornall AO, conducts an independent advisory review of ASIO adverse security assessments (ASAs) furnished to the Department of Home Affairs in respect of eligible persons being persons who:

- remain in immigration detention, and
- have been found by Home Affairs to be owed protection obligations under international law, and
- are ineligible for a permanent protection visa, or have had their permanent protection visa cancelled, because they are the subject of an ASA.

The Independent Reviewer's terms of reference and other relevant information are available at www.ag.gov.au/asarerview.

The Reviewer undertakes a primary review of each adverse security assessment which comes within the terms of reference and periodic reviews every 12 months thereafter while the person remains in detention and ineligible to hold a visa because they are subject to the ASA.

During the course of the year, the Independent Reviewer dealt with adverse security assessments furnished in respect of five eligible persons.

Person 1: During the course of the primary review of this ASA, ASIO furnished a qualified security assessment which replaced the previous adverse assessment. The person's solicitors were advised on 14 July 2020 that the incomplete review had therefore been terminated and, as their client no longer fell within the Independent Reviewer's terms of reference, no further action was required.

Person 2: Person 2's first ASA was furnished on 21 October 2019. While the Independent Reviewer was conducting a primary review, ASIO completed an internal review and furnished a second adverse assessment on 16 July 2020. The review of the first ASA was terminated and a primary review commenced in respect of the second adverse assessment.

During the course of that primary review, the Reviewer advised the Director-General of Security that he may arrive at an opinion that the ASA was not an appropriate outcome.

Following consideration of the Director-General's reply, all of the material ASIO had relied on in making this assessment, other relevant material and information obtained in an interview with Person 2, the Reviewer concluded that a qualified assessment was the appropriate outcome.

The second ASA remains on foot and is due for an annual periodic review by the Independent Reviewer in or about March 2022.

Person 3: Person 3 is the subject of an ASA furnished on 16 October 2019 and a primary review report delivered on 18 May 2020. ASIO commenced an internal review of the ASA in or about March 2021, which had not been completed by the end of the year.

The internal review is expected to result in either a renewed ASA or a qualified security assessment. If there is a new adverse assessment, that ASA will require a primary review by the Independent Reviewer. If the internal review results in a qualified assessment, no further action will be required.

In these circumstances, the annual periodic review of the current ASA, which was due to commence in or about May 2021, has been deferred with the concurrence of Person 3's solicitors as it will be overtaken by the outcome of ASIO's internal review.

Person 4: Person 4 has been the subject of two adverse security assessments which have been reviewed by the Independent Reviewer. The second ASA was furnished by ASIO on 27 October 2020, and the Reviewer's primary review report was delivered on 20 April 2021.

The second ASA remains on foot and is due for an annual periodic review by the Independent Reviewer in or about April 2022.

Person 5: Person 5 is the subject of an adverse security assessment furnished on 20 November 2017, which was the subject of a primary review report delivered on 18 June 2020. That ASA is now due for an annual periodic assessment.

The Independent Review function

This is my last annual report to Parliament. My appointment as Independent Reviewer expires on 26 September 2021. I was initially appointed by the Attorney-General on 3 September 2015 and have continued under successive appointments and contract variations since then except for the period from 2 September 2018 to 27 March 2019, when there were no ASAs requiring independent review.

The Independent Reviewer performs an important function. Refugees who come within the terms of reference can be held in indefinite administrative detention for years without access to judicial review and without being able to return to their home country due to fear of persecution or worse.

Because they cannot change their past, previous actions or associations of security concern will always be on their record. However, the Reviewer is required by the terms of reference to take into account that 'ASIO's security assessments are anticipatory in nature, enabling preventive action to be taken.'

This requirement is consistent with August 2020 *Minister's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its functions and the exercise of its powers*. The guidelines set out governing principles which include:

> 1.8 ASIO's security functions are concerned with threat identification and risk mitigation. These functions are anticipatory in nature.

In several primary reviews, I have agreed with ASIO's assessment of an eligible person's past actions and associations but been uncertain of the basis for the Organisation's assessment of the person's likely future conduct. That assessment may have been simply stated as a finding that the person has 'not demonstrated any change in their extremist ideology' or 'is likely[1] to still hold an ideology supportive of' an extremist organisation.

Those ASAs can reach a stalemate. The person's past stays constant and ASIO remains concerned that they may still hold an extremist ideology and thereby pose a threat to security.

Such a stalemate will result in the person's continued administrative detention until:

- the security environment changes;
- the person is accepted for resettlement in another country; or
- ASIO is able to conclude that the person will not pose a security threat if released into the Australian community.

For this reason, in several primary reviews, I have recommended that ASIO give further and broader consideration to other factors which could influence the person's current ideology and, therefore, their future actions and associations. In making those recommendations I was, of course, aware that consideration of those factors may not change the adverse assessment.

The potentially influential factors I have suggested to ASIO could consider include:

- the person's age and health;
- their family responsibilities;
- if applicable, the person's good behaviour in detention;
- if applicable, the fact that none of their contacts, visitors, email correspondents or internet usage over their years in detention caused any concern;
- their state of mind as revealed in a dynamic psychological assessment;
- the fact that there is no realistic prospect of them being accepted for resettlement in another country and, as a refugee, they cannot return to their home country; and
- that, as a consequence, Australia appears to be their last hope and they would need a strong commitment to an extremist ideology to put the opportunity for them and their family to live in Australia at risk if that opportunity was open to them.

[1] '"Likely" means a circumstance or situation is likely, if the decision-maker is of the opinion that there is a real, and not remote, possibility that the circumstance or situation has occurred, is occurring or may occur': see ASIO's Security Assessment Determination No. 3, paragraph 5.14.2, dated 29 May 2020

I do not doubt that ASIO officers have complied with all statutory and other legal requirements. However, the Independent Reviewer can face difficulty in assessing:

- first, the basis on which ASIO considers that a person continues to hold an extremist ideology; and
- second, the circumstance or situation constituting the anticipated threat that the person poses to the Australian community.

In my view, all of the factors which could reasonably affect the person's current ideology and future threat to security should be taken into account and apparent from the Classified Statement of Grounds provided to the Independent Reviewer.

Appendix J: report on use of questioning warrants and questioning and detention warrants

ASIO is required under section 94 of the ASIO Act to provide in its annual report details of its use of questioning warrants.

Item 18 of Schedule 1 to the *Australian Security Intelligence Organisation Amendment Act 2020* (ASIO Amendment Act) provides that section 94 of the ASIO Act as amended by Part 1 of Schedule 1 to the ASIO Amendment Act applies in relation to annual reports prepared on or after the commencement of item 18.

The details are provided in the following table.

Subsection	Description	2018–19	2019–20	2020–21
94(1)(a)	The total number of requests made during this reporting period under Division 3 (Compulsory questioning powers) of Part III (functions and powers of Organisation) to the Attorney-General for the issue of warrants under that Division (including the number of requests made orally)	0	0	3
94(1)(b)	The total number of warrants issued during this reporting period under Division 3 of Part III (including the number of warrants issued orally)	0	0	3
94(1)(c)	The number of times persons were apprehended during this reporting period under Division 3 of Part III	0	0	0
94(1)(d)	The number of hours each person appeared before a prescribed authority for questioning under a warrant issued during this reporting period under Division 3 of Part III and the total of all those hours for all those persons	-	-	see below
	Person 1			7 hours, 31 minutes*
	Person 2			6 hours, 38 minutes*
	Total hours			***14 hours, 9 minutes***
94(1)(e)	The number of times each prescribed authority had persons appear for questioning before the prescribed authority under warrants issued during this reporting period under that Division	-	-	see below
	Prescribed authority 1	-	-	2

* These hours are a cumulative total of multiple questioning periods for each person

Appendix K: correction of material errors in previous annual report

This appendix corrects the record by explaining reporting errors that occurred in a previous annual report, in accordance with section 17AH(1)(e) of the Public Governance, Performance and Accountability Rule 2014.

The following are corrections to reporting errors made in the *ASIO Annual Report 2019–20*.

On page 61 in Chapter 5 'Management and accountability' under the heading 'Inspector-General of Intelligence and Security', the reporting period for inquiries finalised and recommendations made by the IGIS is incorrectly listed as 2019–20. The correct reporting period was 2018–19. This error did not detract from the substance of the content describing the inspection activities undertaken by the IGIS.

On page 69 in Chapter 5 'Management and Accountability' under the heading 'Consultants', a reporting error was made regarding the total number of new consultancy contracts both in the supporting text and in Table 3. The number of new contractors was incorrectly reported as 27. The correct number of new contractors was 26. This error did not impact the reported expenditure figure of $4 714 610 which was correctly recorded.

On page 71 in Chapter 5 'Management and accountability' under the heading 'Disability reporting' an error was made regarding Appendix E providing workforce statistics on people with a disability. The tables in Appendix E did not report workforce disability data.

A table of workforce disability data is provided below.

	2018–19		2019–20	
People with a disability	21	1.1%	23	1.1%

List of annual report requirements under schedule 2 of the Public Governance, Performance and Accountability Rule

Below is the table set out in Schedule 2 of the Public Governance, Performance and Accountability Rule 2014 (PGPA Rule). Subsection 17AJ(d) of the Rule requires annual reports of Australian Government entities to include this table as an aid of access.

PGPA Rule reference	Description	Requirement	Part of this report
17AD(g)	**Letter of transmittal**		
17AI	A copy of the letter of transmittal signed and dated by accountable authority on date final text approved, with statement that the report has been prepared in accordance with section 46 of the Act and any enabling legislation that specifies additional requirements in relation to the annual report	Mandatory	Letter of transmittal
17AD(h)	**Aids to access**		
17AJ(a)	Table of contents	Mandatory	Preliminaries
17AJ(b)	Alphabetical index	Mandatory	Appendices
17AJ(c)	Glossary of abbreviations and acronyms	Mandatory	Appendices
17AJ(d)	List of requirements	Mandatory	Appendices
17AJ(e)	Details of contact officer	Mandatory	Preliminaries
17AJ(f)	Entity's website address	Mandatory	Preliminaries
17AJ(g)	Electronic address of report	Mandatory	Preliminaries
17AD(a)	**Review by an accountable authority**		
17AD(a)	A review by the accountable authority of the entity	Mandatory	Part 1
17AD(b)	**Overview of the entity**		
17AE(1)(a)(i)	A description of the role and functions of the entity	Mandatory	Part 2
17AE(1)(a)(ii)	A description of the organisational structure of the entity	Mandatory	Part 2
17AE(1)(a)(iii)	A description of the outcomes and programmes administered by the entity	Mandatory	Part 2
17AE(1)(a)(iv)	A description of the purposes of the entity as included in ASIO's corporate plan	Mandatory	Part 2

PGPA Rule reference	Description	Requirement	Part of this report
17AE(1)(aa)(i)	Name of the accountable authority or each member of the accountable authority	Mandatory	Part 2
17AE(1)(aa)(ii)	Position title of the accountable authority or each member of the accountable authority	Mandatory	Part 2
17AE(1)(aa)(iii)	Period as the accountable authority or member of the accountable authority within the reporting period	Mandatory	Part 2
17AE(1)(b)	An outline of the structure of the portfolio of the entity	Mandatory for portfolio departments	Not applicable
17AE(2)	Where the outcomes and programs administered by the entity differ from any Portfolio Budget Statement, Portfolio Additional Estimates Statement or other portfolio estimates statement that was prepared for the entity for the period, include details of variation and reasons for change	Mandatory (if applicable)	Not applicable
17AD(c)	**Report on the performance of the entity**		
	Annual performance statements		
17AD(c)(i); 16F	Annual performance statement in accordance with paragraph 39(1)(b) of the Act and section 16F of the Rule	Mandatory	Part 4
17AD(c)(ii)	***Report on financial performance***		
17AF(1)(a)	A discussion and analysis of the entity's financial performance	Mandatory	Part 4
17AF(1)(b)	A table summarising the total resources and total payments of the entity	Mandatory	Appendices A and B
17AF(2)	If there may be significant changes in the financial results during or after the previous or current reporting period, information on those changes, including the cause of any operating loss of the entity; how the entity has responded to the loss and the actions that have been taken in relation to the loss; and any matter or circumstances that it can reasonably be anticipated will have a significant impact on the entity's future operation or financial results	Mandatory (if applicable)	Not applicable
17AD(d)	**Management and accountability**		
	Corporate governance		
17AG(2)(a)	Information on compliance with section 10 (fraud systems)	Mandatory	Letter of transmittal and Part 5
17AG(2)(b)(i)	A certification by accountable authority that fraud risk assessments and fraud control plans have been prepared	Mandatory	Letter of transmittal

PGPA Rule reference	Description	Requirement	Part of this report
17AG(2)(b)(ii)	A certification by accountable authority that appropriate mechanisms for preventing, detecting incidents of, investigating or otherwise dealing with, and recording or reporting fraud that meet the specific needs of the entity are in place	Mandatory	Letter of transmittal
17AG(2)(b)(iii)	A certification by accountable authority that all reasonable measures have been taken to deal appropriately with fraud relating to the entity	Mandatory	Letter of transmittal
17AG(2)(c)	An outline of structures and processes in place for the entity to implement principles and objectives of corporate governance	Mandatory	Part 5
17AG(2)(d)–(e)	A statement of significant issues reported to the Minister under paragraph 19(1)(e) of the Act that relates to non-compliance with Finance law and action taken to remedy non-compliance	Mandatory (if applicable)	Not applicable
	Audit Committee		
17AG(2A)(a)	A direct electronic address of the charter determining the functions of the entity's audit committee	Mandatory	Exempt
17AG(2A)(b)	The name of each member of the entity's audit committee	Mandatory	Exempt
17AG(2A)(c)	The qualifications, knowledge, skills or experience of each member of the entity's audit committee	Mandatory	Part 5
17AG(2A)(d)	Information about the attendance of each member of the entity's audit committee at committee meetings	Mandatory	Part 5
17AG(2A)(e)	The remuneration of each member of the entity's audit committee	Mandatory	Exempt
	External scrutiny		
17AG(3)	Information on the most significant developments in external scrutiny and the entity's response to the scrutiny	Mandatory	Part 5
17AG(3)(a)	Information on judicial decisions and decisions of administrative tribunals and by the Australian Information Commissioner that may have a significant effect on the operations of the entity	Mandatory (if applicable)	Part 5
17AG(3)(b)	Information on any reports on operations of the entity by the Auditor-General (other than report under section 43 of the Act), a Parliamentary Committee, or the Commonwealth Ombudsman	Mandatory (if applicable)	Part 5
17AG(3)(c)	Information on any capability reviews on the entity that were released during the period	Mandatory (if applicable)	Part 5

PGPA Rule reference	Description	Requirement	Part of this report
	Management of human resources		
17AG(4)(a)	An assessment of the entity's effectiveness in managing and developing employees to achieve entity objectives	Mandatory	Part 5
17AG(4)(aa)	Statistics on the entity's employees on an ongoing and non-ongoing basis, including the following: a. statistics on full-time employees; b. statistics on part-time employees; c. statistics on gender; and d. statistics on staff location.	Mandatory	Appendix C
17AG(4)(b)	Statistics on the entity's Australian Public Service (APS) employees on an ongoing and non-ongoing basis; including the following: ■ statistics on staffing classification; ■ statistics on full-time employees; ■ statistics on part-time employees; ■ statistics on gender; ■ statistics on staff location; and ■ statistics on employees who identify as Indigenous.	Mandatory	Not applicable
17AG(4)(c)	Information on any enterprise agreements, individual flexibility arrangements, Australian workplace agreements, common law contracts and determinations under subsection 24(1) of the *Public Service Act 1999*	Mandatory	Part 5
17AG(4)(c)(i)	Information on the number of SES and non-SES employees covered by agreements etc. identified in paragraph 17AG(4)(c)	Mandatory	Appendix C
17AG(4)(c)(ii)	The salary ranges available for APS employees by classification level	Mandatory	Appendix D
17AG(4)(c)(iii)	A description of non-salary benefits provided to employees	Mandatory	Part 5
17AG(4)(d)(i)	Information on the number of employees at each classification level who received performance pay	Mandatory (if applicable)	Not applicable
17AG(4)(d)(ii)	Information on aggregate amounts of performance pay at each classification level	Mandatory (if applicable)	Not applicable

PGPA Rule reference	Information on aggregate amounts of performance pay at each classification level	Requirement	Part of this report
17AG(4)(d)(iii)	Information on the average amount of performance payment, and range of such payments, at each classification level	Mandatory (if applicable)	Not applicable
17AG(4)(d)(iv)	Information on aggregate amount of performance payments	Mandatory (if applicable)	Not applicable
	Assets management		
17AG(5)	An assessment of effectiveness of assets management where asset management is a significant part of the entity's activities	Mandatory (if applicable)	Not applicable
	Purchasing		
17AG(6)	An assessment of entity performance against the Commonwealth Procurement Rules.	Mandatory	Part 5
	Reportable consultancy contracts		
17AG(7)(a)	A summary statement detailing the number of new reportable consultancy contracts entered into during the period; the total actual expenditure on all such contracts (inclusive of GST); the number of ongoing reportable consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting period on those ongoing contracts (inclusive of GST)	Mandatory	Part 5
17AG(7)(b)	A statement that *'During [reporting period], [specified number] new reportable consultancy contracts were entered into involving total actual expenditure of $[specified million]. In addition, [specified number] ongoing reportable consultancy contracts were active during the period, involving total actual expenditure of $[specified million]'*.	Mandatory	Part 5
17AG(7)(c)	A summary of the policies and procedures for selecting and engaging consultants and the main categories of purposes for which consultants were selected and engaged	Mandatory	Part 5
17AG(7)(d)	A statement that *'Annual reports contain information about actual expenditure on reportable consultancy contracts. Information on the value of reportable consultancy contracts is available on the AusTender website'*.	Mandatory	Part 5

PGPA Rule reference	Description	Requirement	Part of this report
	Reportable non-consultancy contracts		
17AG(7A)(a)	A summary statement detailing the number of new reportable non-consultancy contracts entered into during the period; the total actual expenditure on such contracts (inclusive of GST); the number of ongoing reportable non-consultancy contracts that were entered into during a previous reporting period; and the total actual expenditure in the reporting period on those ongoing contracts (inclusive of GST)	Mandatory	Part 5
17AG(7A)(b)	A statement that *'Annual reports contain information about actual expenditure on reportable non-consultancy contracts. Information on the value of reportable non-consultancy contracts is available on the AusTender website'.*	Mandatory	Part 5
17AD(daa)	***Additional information about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts***		
17AGA	Additional information, in accordance with section 17AGA, about organisations receiving amounts under reportable consultancy contracts or reportable non-consultancy contracts	Mandatory	Part 5
	Australian National Audit Office access clauses		
17AG(8)	If an entity entered into a contract with a value of more than $100 000 (inclusive of GST) and the contract did not provide the Auditor-General with access to the contractor's premises, the report must include the name of the contractor, purpose and value of the contract, and the reason why a clause allowing access was not included in the contract	Mandatory (if applicable)	Not applicable
	Exempt contracts		
17AG(9)	If an entity entered into a contract or there is a standing offer with a value greater than $10 000 (inclusive of GST) which has been exempted from being published in AusTender because it would disclose exempt matters under the *Freedom of Information Act 1982* (FOI Act), the annual report must include a statement that the contract or standing offer has been exempted, and the value of the contract or standing offer, to the extent that doing so does not disclose the exempt matters.	Mandatory (if applicable)	Not applicable
	Small business		
17AG(10)(a)	A statement that *'[Name of entity] supports small business participation in the Commonwealth Government procurement market. Small and medium enterprises (SME) and small enterprise participation statistics are available on the Department of Finance's website'.*	Mandatory	Part 5

PGPA Rule reference	Description	Requirement	Part of this report
17AG(10)(b)	An outline of the ways in which the procurement practices of the entity support small and medium enterprises.	Mandatory	Part 5
17AG(10)(c)	If the entity is considered by the Department administered by the Finance Minister as material in nature—a statement that *'[Name of entity] recognises the importance of ensuring that small businesses are paid on time. The results of the Survey of Australian Government Payments to Small Business are available on the Treasury's website'.*	Mandatory (if applicable)	Part 5
	Financial statements		
17AD(e)	Inclusion of the annual financial statements in accordance with subsection 43(4) of the Act	Mandatory	Part F
	Executive remuneration		
17AD(da)	Information about executive remuneration in accordance with Subdivision C of Division 3A of Part 2–3 of the Rule	Mandatory	Appendix C
17AD(f)	**Other mandatory information**		
17AH(1)(a)(i)	If the entity conducted advertising campaigns, a statement that *'During [reporting period], the [name of entity] conducted the following advertising campaigns: [name of advertising campaigns undertaken]. Further information on those advertising campaigns is available at [address of entity's website] and in the reports on Australian Government advertising prepared by the Department of Finance. Those reports are available on the Department of Finance's website'.*	Mandatory (if applicable)	Part 5
17AH(1)(a)(ii)	If the entity did not conduct advertising campaigns, a statement to that effect	Mandatory (if applicable)	Not applicable
17AH(1)(b)	A statement that *'Information on grants awarded by [name of entity] during [reporting period] is available at [address of entity's website]'*	Mandatory (if applicable)	Not applicable
17AH(1)(c)	Outline of mechanisms of disability reporting, including reference to website for further information	Mandatory	Part 5
17AH(1)(d)	Website reference to where the entity's Information Publication Scheme statement pursuant to Part II of FOI Act can be found	Mandatory	Not applicable (FOI exempt)
17AH(1)(e)	Correction of material errors in previous annual report	Mandatory (if applicable)	Appendix K
17AH(2)	Information required by other legislation	Mandatory	Appendices

List of annual report requirements under other legislation

ASIO is required by section 94 of the ASIO Act to include in its annual report details of its use of questioning warrants; special intelligence operation authorities; authorisations for access to telecommunications data; technical assistance requests, technical assistance notices and technical capability notices; and use of special powers under warrant.

Requirement	Refer to
Statement on questioning warrants	Appendix J
Statement on special intelligence operation authorities	Appendix L
Statement on authorisations for access to telecommunications data	Appendix M
Statement on use of technical assistance requests, technical assistance notices and technical capability notices	Appendix N
Statement on use of special powers under warrant	Appendix O

Consistent with the determination issued to ASIO by the Minister for Finance under section 105D of the *Public Governance Performance and Accountability Act 2013*, appendices L, M, N and O have been deleted from the version of the annual report tabled in parliament to avoid prejudice to ASIO's activities.

Abbreviations and short forms

A

AASB—Australian Accounting Standards Board

AASB 13—Australian Accounting Standards Board Standard 'Fair Value Measurement'

AASB 16—Australian Accounting Standards Board Standard 'Leases'

AASB 119—Australian Accounting Standards Board Standard 'Employee Benefits'

AAT—Administrative Appeals Tribunal

ABF—Australian Border Force

AE—ASIO employee

AEE—ASIO executive employee

AFP—Australian Federal Police

AO—Officer of the Order of Australia

APS—Australian Public Service

ASA—adverse security assessment

ASIO—Australian Security Intelligence Organisation

ASIO Act—*Australian Security Intelligence Organisation Act 1979*

B

C

CCSF—Commonwealth Child Safe Framework

CMT—Crisis Management Team

CPR—Commonwealth Procurement Rules

CSS—Commonwealth Superannuation Scheme

D

DFAT—Department of Foreign Affairs and Trade

E

eLearning—ASIO's intranet-based learning software program

F

FOI Act—*Freedom of Information Act 1982*

G

GST—goods and services tax

H

HUMINT—human intelligence

I

IGIS—Inspector-General of Intelligence and Security

Independent Reviewer—Independent Reviewer of Adverse Security Assessments

INSLM—Independent National Security Legislation Monitor

ISIL—Islamic State of Iraq and the Levant

ITIL—Information Technology Infrastructure Library

J

K

L

M

N

NABERS—National Australian Built Environment Rating System

O

P

PBS— Portfolio Budget Statement

PGPA Act—*Public Governance, Performance and Accountability Act 2013*

PGPA Rule—Public Governance, Performance and Accountability Rule

PJCIS—Parliamentary Joint Committee on Intelligence and Security

PSS—Public Sector Superannuation Scheme

PSSap—Public Sector Superannuation accumulation plan

Q

R

S

SES—Senior Executive Service

SME—small and medium enterprises

SMMA—Service Management Maturity Assessment

T

U

US—United States

V

W

X

Y

Z

Glossary

adverse security assessment—ASIO recommends a prescribed administrative action that would be prejudicial to the interests of a person be taken or not taken, such as the refusal of a visa or cancellation of a passport

communal violence—violence between different groups or individuals in the Australian community that endangers the peace, order or good government of the Commonwealth

espionage—the theft of Australian information or capabilities for passage to another country, which undermines Australia's national interest or advantages a foreign country

foreign fighter—an individual who leaves their home country to join or train with a violent extremist group in an armed conflict overseas

foreign interference—clandestine, deceptive or threatening activity conducted on behalf of a foreign power which aims to affect political or governmental processes or is otherwise detrimental to Australia's interests

foreign power—a foreign government, an entity that is directed or controlled by a foreign government or governments, or a foreign political organisation

investigation—the processes involved in collecting, correlating and evaluating information about individuals, groups or other entities in order to understand known security threats or identify emerging ones

malicious insiders—trusted employees or contractors who deliberately breach their duty to maintain the security of privileged information, techniques, technology, assets or premises

non-prejudicial security assessment—ASIO does not have security concerns about a proposed administrative action, such as the granting of a visa or issuing of a passport

qualified security assessment—ASIO does not make a prejudicial recommendation concerning a prescribed administrative action, but communicates information or advice that is, or could be, prejudicial to the interests of a person in relation to that action

radicalisation—the process by which an individual's beliefs move away from a rejection of violence to achieve societal or political change towards an endorsement or promotion of violence to achieve that change

sabotage—damaging or disruptive activity against infrastructure—including electronic systems—to undermine Australia's national security or advantage a foreign power. Acts of sabotage are not limited to irreversible, destructive attacks on physical infrastructure; they can include small-scale, selective and temporary acts of degradation or disruption to networked infrastructure

terrorism—a tactic employed by a group or individual that involves the use of violence to achieve or advance a political, religious or ideological goal

violent extremism—includes *ideologically motivated violet extremism* which denotes support for violence to achieve political outcomes or in response to specific political or social grievance/s and *religiously motivated violent extremism* which denotes support for violence to oppose or achieve a specific social, political or legal system based on a religious interpretation

Index

W

Y

Z

10,2
18,17
45,18
23,7
103,60
116,24
85,23
93,4
75,9
150,18

asio.gov.au