IGIS

INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY

Mrs Lucy Wicks MP
Chair
Joint Committee of Public Accounts and Audit
Email: jcpaa@aph.gov.au

Dear Mrs Wicks

I welcome the opportunity to make this submission to the Joint Committee of Public Accounts and Audit's inquiry into matters contained and associated with the Auditor-General's Report No.11 of 2019-20 *Implementation of the Digital Continuity 2020 Policy* (the Report), published on 31 October 2019, particularly those parts of the Report which relate to the Office of the Inspector-General of Intelligence and Security (IGIS).

The Report presented the findings and recommendations of the Australian National Audit Office's (ANAO) audit into the extent to which three Australian Government agencies – IGIS, the Attorney-General's Department (AGD) and the Civil Aviation Safety Authority (CASA) – implemented the Government's *Digital Continuity 2020* (DC 2020) policy. The audit also examined how effectively the National Archives of Australia monitored, assisted and encouraged entities to meet the policy's specified targets.

With regard to IGIS, the Report acknowledged the Office's progress in implementing aspects of DC 2020, and noted some of the external security requirements that limit IGIS's ability to satisfy fully certain principles of DC 2020. Of particular relevance is Recommendation 7 (paragraph 4.67), which stated that IGIS should "establish a plan for the implementation of the Digital Continuity 2020 policy, with a particular focus on those targets which were due on or before the end of 2018. The plan should…include clear processes for ongoing monitoring and reporting of progress".

My predecessor as Inspector-General, the Hon Margaret Stone AO, FAAL, agreed to implement this recommendation. In a letter to the Auditor-General for Australia, Mr Grant Hehir, on 2 September 2019, Ms Stone noted that due to "an appropriation of…funds to implement recommendations from the 2017 Independent Intelligence Review,…for the first time this office now has some resources to dedicate to the implementation of DC2020 targets". The full text of this letter is attached at Attachment A.

IMPLEMENTATION OF DC 2020

In the 15 months since the Report was published, IGIS has made good progress in implementing Recommendation 7, and DC 2020 more broadly. This includes a establishing a plan to implement DC 2020. I will discuss this plan shortly, but would first like to note IGIS's current status and how this has evolved since the 2017 Independent Intelligence Review and its associated injection of funds. This context is important to understanding IGIS's approach to implementing Recommendation 7 and DC 2020. Until 2017 IGIS was very small, with limited

resources. Since that time, we have grown quickly, doubling in size between 2018 and 2020, and are funded to grow to 55 ASL. More detail on IGIS's roles and responsibilities can be found at <u>Attachment C</u>.

DC 2020 TARGETS: ANAO FINDINGS AND IGIS SOLUTIONS

The Report measured the progress of IGIS, AGD and CASA against targets under the three key principles of DC 2020, which were:

1. *Information is valued – agencies will* **manage their information as an asset**, *ensuring that it is created and managed for as long as required, taking into account business and other needs and risks.*
2. *Information is managed digitally – agencies will transition to* **entirely digital work processes**, *meaning business processes including authorisations and approvals are completed digitally, and that information is created and managed in digital format.*
3. *Information, systems and processes are interoperable – agencies will have* **interoperable information, systems and processes** *that meet standards for short and long term management, improve information quality and enable information to be found, managed, shared and reused easily and efficiently.*

IGIS has implemented the Report's Recommendation 7 as follows.

The first step was IGIS's engagement of KPMG in October 2019 to design a governance framework suitable for an expanded agency, to replace the legacy and ad hoc arrangements (including those relating to information governance) then in place. KPMG's report was finalised by April 2020; amongst its 15 recommendations were three of particular relevance to IGIS's information governance planning:

- *Increase the number of resources to implement and provide oversight of governance functions including secretariat, risk and compliance.*
- *Implement clearly devolved responsibility and accountability, but with more consultation across the agency....Specific resources will be required to manage better practice governance.*
- *Increase the frequency of key governance functions such as internal audit committee meetings, strategic planning and performance reviews.*

These recommendations informed IGIS strategic planning as the Office returned to full operational capacity in mid-2020 after several months of COVID-related disruption. This disruption meant that some work on information governance was necessarily delayed.

Central to IGIS's planning has been a reorganisation to better meet the increased demands of a growing agency. The restructure commenced in August 2020 and was completed in December 2020. This now means IGIS will have a dedicated area focussing on information governance, and recruitment is currently under way.

We have also engaged an experienced information governance specialist, who was tasked with the following actions:

- Review IGIS's current information governance architecture and practices, and assess the extent to which these are fit for purpose (completed December 2020);
- Develop a plan for implementing ANAO recommendation 7 and DC 2020 more broadly (completed December 2020 – see below); and

Official

- Develop an Information Governance Framework for updating and managing IGIS's architecture and information holdings, in accordance with Commonwealth information management policies and across electronic and hard copy systems and a range of classification levels (under way).

In addition, the IGIS Executive has implemented initiatives to devolve responsibility, clarify accountability, and improve consultation across the Office. This includes in relation to information governance and digital record-keeping.

NEXT STEPS

Since ANAO's Report was published in October 2019, IGIS is (notwithstanding the unexpected events of 2020) developing and implementing a coherent strategy to address Recommendation 7, including through the DC 2020 implementation plan developed by our information governance specialist. The plan contains the following five key actions:

1. **Develop an Information Governance Framework for IGIS.** This is in train and due for completion by May 2021.
2. **Ensure IGIS's risk framework addresses information management.** This action is being addressed through a review of IGIS's risk management framework that is under way.
3. **Establish a reporting mechanism to manage compliance, risk and business needs.** This is being developed as part of the Information Governance Framework, and other processes already under way.
4. **Update all relevant policies so they are fit for purpose for a digital environment.** This includes both internal policies and external agreements.
5. **Nurture a culture that values knowledge management.** This includes training to ensure IGIS staff know what is required of them in terms of information management. This work has already commenced, and will be ongoing.

A copy of the implementation plan is attached at Attachment B.

Thank you again for the opportunity to provide this submission.

Yours sincerely

Dr Christopher Jessup QC
Inspector-General

25/2/21

Official

Official

ATTACHMENT A

IGIS
INSPECTOR-GENERAL of
INTELLIGENCE AND SECURITY

File ref: 2019/003
Correspondence ref: OIGIS/OUT/2019/823

Mr Grant Hehir
Auditor-General for Australia
C/O: Electronic mail

Dear Mr Hehir

Letter of Reply – Implementation of the Digital Continuity 2020 Policy

Thank you for your correspondence on 05 August 2019 which contained the *Proposed Report for the ANAO Performance Audit – Implementation of the Digital Continuity 2020 policy*. I have reviewed the report and provide the following comments and attachments.

Recommendation no. 7 of your report relates to my agency, and the establishment of a plan for the implementation and reporting of Digital Continuity 2020 (DC 2020) targets. I accept that recommendation.

In 2018, this agency received an appropriation of both capital and operating funds to implement recommendations from the 2017 Independent Intelligence Review, meaning that for the first time, this Office now has some resources to dedicate to the implementation of DC2020 targets. I note that due to the security requirements of this office, there are some elements of the DC2020 policy which will not be able to be implemented (examples of which were provided during the audit process).

The contact in my office for this matter is the Deputy Inspector-General, Mr Jake Blight, who can be contacted by telephone on ███████ or email: ███████████

Yours sincerely

████████████

Margaret Stone AO, FAAL
Inspector-General

2 September 2019

Attachments:
1. Summary Response
2. Editorial Matters

Official

Official

IGIS
INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY

ATTACHMENT B

IMPLEMENTING DC 2020:

DEVELOPING AN INFORMATION GOVERNANCE FRAMEWORK FOR IGIS

Prepared December 2020

Introduction

1. The Office of the Inspector-General of Intelligence and Security (IGIS, or the Office) has a strong recordkeeping discipline in the hardcopy environment. To comply with the requirements of National Archives of Australia's (NAA's) policies *Digital Continuity 2020* policy (DC 2020, which concluded on 31 December 2020) and its successor policy *Building Trust in the Public Record* policy, IGIS recordkeeping must be modernised to progress to a fully digital environment. The Office needs to calibrate its thinking of information governance to be broader than recordkeeping, which will be facilitated through the development of the Information Governance Framework – our plan to implement DC 2020.

2. IGIS has developed this plan in response to Recommendation 7 of the 31 October 2019 ANAO report *Implementation of the Digital Continuity 2020 Policy* (the report). The report highlighted a number of areas to be targeted for improvement, and requested an implementation plan be developed for the elements of DC 2020 that had fallen due on 31 December 2018. This document constitutes the plan recommended in Recommendation 7.

NAA and DC 2020

3. The purpose of the NAA's whole-of-government DC 2020 initiative was to require agencies to review their information governance arrangements to support the Government's digital transformation initiatives that are driving e-government. The process was designed to help agencies realise fully the benefits of their information assets and how the assets can support agencies undertake their core business, and for the government to deliver a better and more efficient service to Australians.

4. There are three main principles in the DC 2020 policy:

    - Information is valued

    - Information is managed digitally, and

    - Information, systems and process are interoperable.

5. DC 2020 covers the information governance framework as well as policies, processes, standards, controls and reporting metrics to ensure that business, information management, and legislative requirements are met and risk is managed.

Official

Official

6.   As part of the "information is managed digitally" DC 2020 principle, there is a requirement to assess business systems against their ability to meet NAA requirements.   The IGIS uses commercial off-the-shelf (COTS) products that meet the functional requirements for information management.   A DC 2020 target is to evaluate business systems against the NAA's business systems assessment framework. This activity will be completed in the scope of this work to ensure IGIS systems continue to meet whole of government information management requirements.

7.   DC 2020 will be superseded on 1 January 2021 by the new NAA whole-of-government policy *Building Trust in the Public Record: Managing Information and Data for Government and Community (Building Trust)*.   Once the Office has met the requirements of DC 2020 it can commence implementation of *Building Trust* – although many of this policy's compulsory components will be covered by the activities outlined in this plan.

Priority action areas

8.   Five main areas have been identified as critical to the development of an Information Governance Framework (the framework) and for the implementation of DC 2020 targets for IGIS. Priority areas are outlined below.

8.1.   Information Governance Framework

The primary activity in this work program is the development of an information governance framework for IGIS. The framework will define the fundamental approach of IGIS to managing and valuing its information assets.

The framework will make linkages to broader IGIS governance, and support the Office in achieving its core objectives.

It will also incorporate planning activities that relate to business continuity, risk and corporate planning.

A key cultural element of the framework will be to define the responsibilities of all staff in relation to information management. This will cover the creation, capture and lifecycle management of the Office's information.

To support all aspects of the framework, key drivers and what information means to the Office will be defined.

8.2.   Risk

Within the office, a review of the risk management framework is being planned by governance specialists. The information governance work will complement this review, which will see information governance, and information management included as its own risk. The relationships and dependencies on other identified risks will also be made.

Official

Official

8.3.   Reporting

As identified by the ANAO report, current reporting in information governance should be more frequent and formalised. The reporting will assist IGIS to manage compliance, risk and business needs as they relate to information governance and information management.

8.4.   Policies

IGIS has existing information management policies that require updating to reflect the move to the digital environment. The updates will commence once a mature draft of the framework is developed.

There is also a requirement for the development and/or review of implementation and guidance documentation in the form of standards and guidelines to assist IGIS staff to continue to meet their information management obligations relating to Commonwealth records.

8.5.   Knowledge Management

As part of the information governance framework activities, a training plan will be developed to maintain high levels of skill across the IGIS in information governance, knowledge management and information management. This will contribute to the further development of IGIS's current knowledge management and will assist with developing a scalable approach as the agency's growth occurs and ensure consistent advice to all staff and application of IGIS core activities when working with other agencies.

Timeframe

9.   IGIS already has some information governance documentation that falls within the parameters of the five themes outlined above. However, these documents have evolved ad hoc, are not contemporary and do not constitute a coherent framework.

10.   The work of the information specialist on an information governance framework for the IGIS aims to be finalised no later than May 2021. The framework will address any outstanding obligations IGIS has in relation to DC 2020 (notwithstanding that policy's expiry on 31 December 2020), and positions the Office to quickly begin implementation of the *Building Trust* policy.

11.   Once IGIS has an agreed framework, it will identify, prioritise and set deadlines for finalising discreet bodies of work within the framework. Mechanisms for review will be built into the framework to ensure timely adjustments as required by law or changes in whole of government approach.

12.   The IGIS Executive prioritises effective and efficient information governance and the need to embed these values in day-to-day work.

Official

ATTACHMENT C

ABOUT IGIS

IGIS is an independent statutory agency within the Attorney-General's portfolio. As at 8 February 2021, IGIS had 34 staff employed under the *Public Service Act 1999*, in addition to the Inspector-General. The Inspector-General is an independent statutory officer appointed under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act). The Hon Dr Christopher Jessup QC commenced as the Inspector-General on 8 February 2021 (having been Acting Inspector-General since 18 January 2021).

Under its existing jurisdiction, IGIS reviews the activities of the following six intelligence agencies:
- Office of National Intelligence (ONI)
- Australian Security Intelligence Organisation (ASIO)
- Australian Secret Intelligence Service (ASIS)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO), and
- Defence Intelligence Organisation (DIO).

The overarching purpose of IGIS's activities is to provide assurance that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights.

As the IGIS Corporate Plan sets out, the approach IGIS takes to its role is:
- independent and impartial ('we select what to look at and how to look at it');
- astute and informed ('we know what agencies are doing and why');
- measured ('we focus on serious and systemic issues');
- open ('we are open about our approach to oversight'); and
- influential ('we assist agencies to improve their compliance').

A significant proportion of the resources of IGIS are directed towards ongoing inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action. IGIS has a risk-based approach to its inspection program, targeting high risk activities and activities with the potential to affect the lives or rights of Australian citizens detrimentally. Accordingly, the IGIS inspection program mainly focuses on the activities of agencies with intrusive powers and investigative techniques. IGIS also takes into account an agency's internal control mechanisms as well as its history of compliance and reporting. Section 35 of the IGIS Act requires the Inspector-General to report annually on inspections conducted during the year.

The inspection role of IGIS is complemented by an inquiry function. The IGIS Act provides that the Inspector-General may conduct an independent inquiry into the activities of an intelligence agency either on the Inspector-General's own motion, at the request of a Minister, or in response to a complaint. The Prime Minister can request the Inspector-General to conduct an inquiry into an intelligence or security matter relating to any Commonwealth agency.

In undertaking inquiries, the Inspector-General has strong investigative powers, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve classified or sensitive information, and the methods by which it is

Official

collected. Conducting an inquiry is resource intensive but provides a rigorous way of examining a complaint, serious incident or systemic matter within an agency. At the conclusion of an inquiry, the Inspector-General provides a report with findings and recommendations to the responsible Minister. Where an inquiry is in response to a complaint, a written response is given to the complainant. Where possible, an unclassified report or summary is published on the IGIS website.

Finally, the Inspector-General receives and investigates complaints about the six intelligence agencies within the Inspector-General's jurisdiction. Complaints can be made by a member of the public, or by a current or former employee of an intelligence agency, about the activities of an intelligence agency. IGIS also receives and, where appropriate, investigates public interest disclosures about suspected wrongdoing within the intelligence agencies. With IGIS's access to the records of intelligence agencies and ability to examine the full set of circumstances of any complaint, complaints and other matters can often be quickly resolved. Where there are issues requiring further investigation, the Inspector-General can conduct a formal inquiry into the complaint. Details about individual complaints and their resolution are not made public. However the complainant is always provided with as much information about the outcome as possible, within security restrictions.