Australian Government
Geoscience Australia

SUBMISSION TO THE INQUIRY BASED ON: ANAO REPORT No.53 (2017-18) *CYBER RESILIENCE*

Terms of Reference

The Joint Committee of Public Accounts and Audit (JCPAA) has commenced an inquiry based on ANAO Audit Report No.53 (2017-18), Cyber Resilience. Geoscience Australia have been requested by the JCPAA to make a submission to the inquiry, including:

- An implementation status update on the audit recommendations directed at your agency.
- An outline of future plans and milestones for actions that are still to be completed.
- Other related matters, such as changes made due to audit findings (but not specifically recommended in the audit) or other relevant activity by the agency.

Key Points

- The Australian National Audit Office (ANAO) Report No.53 (2017-18) *Cyber Resilience,* directed one recommendation at Geoscience Australia: '*Geoscience Australia and National Archives of Australia each establish a plan and timeframe to achieve compliance with the Top Four mitigation strategies, and monitor delivery against that plan*'.
- In response to this recommendation, a Security Strategy 2018-2020 (the Strategy) and roadmap were developed. The roadmap provides guidance on how we will address cyber resilience across three key focus areas:
    - People and Culture;
    - Technical Controls; and
    - Security Governance.
- To facilitate the implementation of the Strategy and roadmap, a Security Improvement Program (SIP) has been established. The SIP is internally funded and scheduled for completion in June 2020.
- The Strategy and SIP provide the foundation of cyber resilience for Geoscience Australia which:
    - Implements the Australian Cyber Security Centre (ACSC) Essential Eight including the Top Four Strategies to Mitigate Cyber Incidents (Top Four):

        - Application whitelisting;
        - Patching applications;
        - Patching operating systems;
        - Restrict administrative privileges;
        - Configure Microsoft Office macro settings;
        - User application hardening;
        - Multi-factor authentication; and
        - Daily backups.

      The four non-mandatory strategies of the Essential Eight will be configured appropriately by using a risk based approach and the Essential Eight Maturity Model.

    - Establishes a standardised security architecture and control framework for Information and Communication Technology (ICT) across the organisation to deliver a service-orientated model that enables business to be secure and resilient;
    - Enhances existing security and risk governance processes and supports these processes through the implementation of contemporary technical controls that are practical, identify and support the management of cyber security risks and contribute to the integrity of organisational information and systems;
    - Improves resilience for essential business systems and services with respect to availability, recoverability and resistance to attack. These include:
        - User workstations;
        - Authentication services; and
        - Email servers.
    - Establishes education and awareness strategies that promote the importance of security and cyber resilience and fosters a security aware culture through the delivery of a series of staff information sessions, working groups, enhanced internal resources and new policies and procedures.

- The following outcomes have been delivered by the SIP to date:
    - Extensive stakeholder consultation and assessment of the current state of the ICT environment;
    - Development, cost analysis and approval of the SIP business case, including a significant investment of resources to fund the uplift of cyber resilience;
    - Identification and commencement of staff resources for the SIP and sustainment activities post-SIP completion;
    - Development and implementation of an extensive communications and awareness strategy to assist in organisational change management and enhancing security awareness This will be ongoing to keep the messages prominent;
    - Development and endorsement of a new ICT Security Policy and Procedures;
    - Delivery of multiple security awareness and information sessions for all employees;
    - Successful trial of an application whitelisting solution that will be deployed within our ICT environment by 30 June 2019;
    - Implementation of application whitelisting in audit mode that has collected detailed information on software that is operating on user workstations, leveraging a recently developed workstation hardened Standard Operating Environment (SOE) and a hardware refresh for Windows 10 devices;
    - Development of a security documentation framework;

- Increased visibility of managed service provider services including operating system patching and administrative account management through the establishment of additional targeted reporting;
- Establishment of automated health check reports for administrative and user account management; and
- Establishment of a Security Technical Working Group to facilitate a collaborative approach with business and subject matter experts.

Geoscience Australia has taken a risk-based approach aligned with the Top Four and Essential Eight guidance for prioritisation of activities. The practical application of this approach is a focus on delivering capabilities, which are initially applied to essential business systems and services. Once the capability is established and implemented, future plans and milestones include the following actions:

- An application whitelisting capability will be comprehensively implemented on these systems by 30 June 2019, with non-essential systems and services to be remediated by 30 June 2020.
- Projects scheduled for completion by the end of the SIP, in addition to the Top Four and Essential Eight, include:
  - Vulnerability Management – to reduce our exposure to cyber attack;
  - Governance and Architecture – to enable our business to be more secure and resilient within a service-orientated security model;
  - People and Culture – to foster a culture of security awareness and resilience; and
  - Technical Controls – to prevent the compromise of and ensure the availability and integrity of our information and systems.

Other related matters, such as changes made due to audit findings (but not specifically recommended in the audit) or other relevant activity by Geoscience Australia include:

- Successful upgrade of “Endpoint security” software on the workstation fleet providing advanced threat detection capabilities;
- Trialling a cloud application security product to monitor usage of cloud products and file sharing behaviours with the intent of a risk-based assessment and determination of any changes necessary to ensure the secure adoption of cloud services;
- Commencement of a proof of concept for an email sandboxing solution that will strengthen our ability to block malicious content;
- The implementation of increased threat detection capabilities in November 2018 with over 35 new detection patterns created in an existing security information and event management tool; and
- Increased physical security awareness such as educational videos on escorting visitor requirements displayed on digital screens throughout the premises. This was communicated to staff through multiple channels.

Background

Geoscience Australia is Australia's pre-eminent public-sector geoscience organisation and the nation's trusted adviser on the geology and geography of Australia. It applies science and technology to describe and understand the Earth for the benefit of Australia.

Geoscience Australia delivers a wide range of products and services that address important national issues to assist government and the community to make informed decisions about the use of natural resources, the management of the environment, and community safety.

Geoscience Australia was subject to an ANAO audit on Cyber Resilience, with the subsequent report published on 28 June 2018. There was one recommendation from the audit directed at Geoscience Australia, and several supporting findings.

Geoscience Australia is actively addressing the recommendation and findings from the ANAO audit and provides the key points in this document as submission in relation to the terms of reference provided.

Attachments:
'Security Strategy 2018-2020.pdf'

Australian Government
Geoscience Australia

GEOSCIENCE AUSTRALIA SECURITY STRATEGY 2018–2020

Geoscience Australia's security strategy supports the One GA vision and aims to protect our people, property, information and reputation while enabling business.

- We will protect our people by exercising our duty of care to staff and visitors
- We will protect our information and systems with risk-based controls to ensure its integrity, confidentiality and availability
- We will protect our assets and resources using a risk-based approach
- We will support our business and reputation by applying appropriate levels of controls and governance

Pursuing Science Excellence	Maximising Data Potential	Ensuring Supportive Stakeholders	Fostering a Positive Organisational Culture
Supporting secure and controlled information sharing	Ensuring the integrity and availability of data and systems	Implementing governance to provide accountability and stakeholder assurance	Educating our people in security and risk to support the One GA vision

WHERE WE ARE NOW	ACTIONS	WHERE WE WANT TO BE

PEOPLE AND CULTURE
• We have no clearly communicated security strategy or documented security outcomes
• Our staff are not equipped with the appropriate tools and processes to effectively perform their job and meet security requirements
• Security is often considered too late in the business process and risk is not routinely assessed
	• Deliver a change management and cultural improvement framework, covering:
	  ○ communications
	  ○ education and awareness
	  ○ staff roles and responsibilities
	  ○ executive support
		• An improved security awareness culture defined by an educated and knowledgeable workforce
		• An established security framework empowering employees with readily available and accessible security information, processes and support
		• A security team that proactively assists the business in delivering organisational outcomes

TECHNICAL CONTROLS • We have not implemented or consistently applied appropriate technical controls and procedures • Our information and systems risks are not sufficiently controlled • Security exemptions lead to increased risk exposure • Our people, physical assets and resources are generally adequately protected	• Implement risk-based controls and procedures to ensure compliance with recommended security requirements • Implement controls and procedures to ensure compliance with mandatory security requirements • Continue regular reviews and updates of physical security	• Improved protection for our information, assets and reputation • Risk-based controls that support business operations and reduce risks to tolerable levels • Progress the implementation of a robust and secure network to effectively mitigate security risks • Compliance with government mandatory security requirements
SECURITY GOVERNANCE • Our decisions do not always support secure outcomes as relevant information is not always available • We have a limited understanding of our security environment due to inadequate monitoring and reporting • Our staff do not clearly understand their roles and responsibilities relating to security	• Undertake business impact assessments and risk reviews to prioritise security effort • Review resourcing and governance structures to align with strategic direction and business requirements • Continue maturing the security governance framework comprising policy, procedures and plans • Improve the security monitoring and reporting framework	• Security risks are assessed, understood and accepted at the appropriate level • Enhanced transparency and visibility of information to aid risk-based decision making • Staff roles and responsibilities are clearly established, understood and supported • Effective monitoring, reporting and assurance arrangements are in place