Privacy Threshold Assessment

Project Details

Project name	Electronic Access Control System (EACS) and Closed-Circuit Television (CCTV) Upgrade – Symonston and Alice Springs sites
Business owner	Manager, Facilities (Finance and Facilities)
Threshold assessment drafter	Project Manager (Program Management and Delivery)
Description of the project	The current EACS and CCTV systems in Geoscience Australia's Symonston building have been in operation for a considerable time and need to be upgraded and replaced before they reach their end of life. The existing EACS also controls access to Geoscience Australia's Alice Springs site remotely and this functionality will be retained. The system at Alice Springs will continue to be monitored off-site by a third party security provider. The project will replace the existing systems, upgrade some CCTV cameras and install additional cameras at Symonston to provide perimeter security. Where new cameras are added, suitable signage related to the recording / monitoring of activities will be posted across the site. There will be no changes to CCTV in the Alice Springs site. Key objectives of these new systems are to: • Secure building perimeters from potential threats and intrusions • Provide a physically safe and secure environment for staff and visitors, including in an emergency • Comply with the Protective Security Policy Framework (PSPF), Australian Information Security Manual and ASIO Technical Notes 1/15 and 5/12 in terms of physical, information and personnel security • Comply with other regulations such as *Archives Act 1983*, IEC 60389 access control, Building Code (where relevant), ACT Fire Safety standards and legislation, Geoscience Australia's security strategy and roadmap and CCTV Procedure.
Types of personal information being handled as part of the project	No 'new' information about people will be stored in the EACS system. The current system stores individuals' names and their access information to the building. The minimum amount of personal information to effectively operate the EACS is collected. The new CCTV cameras will have the potential to identify people through their images to the same extent as those already in place. Potentially, this may include sensitive information, for example, where an individual's racial or ethnic origin (or an opinion about this) can be derived from the image.

What is the purpose of handling the personal information?	Personal information collected via the EACS and CCTV enables Geoscience Australia to take appropriate action in relation to suspected unlawful activity or serious misconduct that may be engaged in. These systems assist the entity to meet its PSPF requirements to implement appropriate security measures to protect its people, information and assets. Images collected from the CCTV system will be stored for 180 days in an onsite stand-alone system and will be accessible to those that have a need to know and are authorised for security-related matters as covered in the CCTV Procedure. This includes designated roles within Geoscience Australia and security officers contracted under whole-of-Australian-Government property services arrangements. In addition, Geoscience Australia will provide the contractor installing the new system with data from the current system to load into the new system. These third parties are contractually required to comply with the Australia Privacy Principles (APPs). Personal information may be provided to enforcement bodies to investigate suspected unlawful activity or serious misconduct.
Stakeholders	The following teams / staff have been engaged during this project: Director, Governance Entity Security Advisor Director, Cyber Security Director, Digital Science Infrastructure and Integration Manager, Facilities Director, Program Management and Delivery SCEC Consultant Evolve Facilities Management

Part 1: Personal information handling

Does the project involve new or changed ways of handling personal information?

☐ **Yes** Complete Part 2 of the assessment below.

☑ **No** It is not necessary to complete a privacy impact assessment (PIA).
Record the decision at Part 3 and file this assessment with the Privacy Officer.

Part 2: Determining potential for a high privacy risk

Consider the following questions and record each answer as 'yes', 'potentially' or 'no'. The purpose of these questions is to you help you screen for factors which point to the potential for a high privacy risk project. It's important to note that these questions are non-exhaustive, and you should also consider whether there are any other relevant factors that may indicate that your project is a high privacy risk project.

Will the project involve:	Yes	Potentially	No
Handling large amounts of personal information? *Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.*	☐	☐	☑
Handling sensitive personal information? *Sensitive personal information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual preferences or practices, biometric information, health information and genetic information.* *The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).*	☐	☑	☐
Sensitivities based on the context in which the project will operate? *Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?*	☐	☐	☑
Handling personal information in a way that could have a significant impact on the individuals concerned? *Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft.*	☐	☐	☑
Disclosing personal information outside of your entity? *Consider whether your project will involve sharing personal information with another entity, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas.*	☑	☐	☐

Will the project involve:	Yes	Potentially	No
Handling personal information of individuals who are known to be vulnerable? *Consider whether the activity may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.* *An individual's circumstances, or the increased power imbalance between the individual and an entity, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.*	☐	☐	☑
Using or disclosing personal information for profiling or behavioural predictions? *This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).*	☐	☐	☑
Using personal information for automated decision-making? *This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.*	☐	☐	☑
Systematic monitoring or tracking of individuals? *For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.*	☐	☐	☑
Collecting personal information without notification to, or consent of, the individual? *This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.*	☐	☐	☑
Data matching (linking unconnected personal information)? *For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources.*	☐	☐	☑
Any other relevant factors that may have a significant impact on the privacy of individuals?	☐	☐	☑

Part 3: Decision & declaration

If you have answered 'Yes' or 'Potentially' to any of the questions in Part 2, a PIA should be completed. If you are uncertain as to whether you have considered all relevant risks, you are strongly encouraged to seek support from the Privacy Officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

☐ **Yes** Yes, there are (or potentially are) high privacy risk elements to this project.

☑ **No** No, a PIA is not necessary. The project does not carry any high privacy risks.

The new EACS and CCTV system does not fundamentally change the existing practices for handling personal information. The collection, use and disclosure of personal information (and potentially sensitive information) by these systems is reasonably necessary to enable Geoscience Australia to take appropriate action in relation to suspected unlawful activity. Whilst personal information wll be used by and/or disclosed to third parties involved in the installation and ongoing monitoring of the systems, the contractual and procedural controls in place to protect personal information are proportionate to the risks.

Business owner sign-off

Position	Manager, Facilities	Date	20/05/2022

Privacy Officer sign-off

Position	Director Engagement, Commercial and Legal	Date	20/05/2022