SUPERANNUATION ECOSYSTEM

Cyber Security Incident Response Discussion Exercise

April 2026

Overview

Building on the success and insights gained from three consecutive ecosystem exercises, the Gateway Network Governance Body (GNGB) is inviting ecosystem participants to register their interest in the **2026 Superannuation Ecosystem Cyber Incident Response Exercise.**

Australia's superannuation system is globally recognised and forms a critical pillar of the financial services sector, safeguarding the retirement savings of millions of Australians. As cyber threats continue to increase in frequency, scale and sophistication, the ecosystem faces heightened risks that extend beyond individual organisations to the stability of the broader financial system and public confidence.

The highly interconnected nature of the superannuation ecosystem means that a cyber incident impacting one entity can rapidly propagate across the network, creating potential systemic consequences. Over the past three exercises, participation and engagement across the ecosystem have continued to grow, reinforcing the value of a coordinated approach to testing and strengthening cyber resilience.

Exercising together enables organisations to better understand interdependencies, identify critical coordination points, and collaborate on strategies to mitigate risks to the superannuation system and its members.

The aim of the 2026 exercise is to further explore how organisations within Australia's superannuation ecosystem prepare for and respond to a significant cyber security incident. It will support participants to identify where response and recovery plans align, where they diverge, and where opportunities exist to strengthen collective capability.

If you are interested in collaborating with peers across the superannuation ecosystem to enhance both individual and collective cyber response readiness, the following outlines the proposed approach and program of work. We look forward to continuing this important initiative with you.

Exercise Outline

The cyber security exercise for Australia's superannuation ecosystem will be delivered as a facilitated tabletop discussion. Participants will work through a simulated scenario, enabling in-depth exploration of key issues and coordinated verbal responses to evolving events.

Throughout the exercise, participants will be presented with a series of progressively complex scenario developments (referred to as "injects") designed to guide discussion, test decision-making, and explore response strategies as the incident unfolds.

Participation

We are inviting a diverse range of organisations from across the superannuation ecosystem to participate. To ensure an appropriate mix of participants, submission of an expression of interest does not guarantee inclusion; however, we will endeavour to accommodate all interested organisations where possible.

Each selected organisation will be offered participation for up to two exercise participants and one planner.

The Planner Role

The planner role is integral to the success of the exercise, contributing to the development of a scenario that is both realistic and aligned to the exercise objectives. Planners will form part of the Exercise Planning Group, which is responsible for the following activities:

- Developing the exercise aim and objectives
- Designing the scenario and supporting injects
- Managing internal planning and administrative activities
- Supporting the evaluation of the exercise

Each participating organisation will be offered one place in the Exercise Planning Group. The nominated individual should have a strong understanding of the threat landscape facing the ecosystem, as well as familiarity with their organisation's incident response and recovery processes.

Please provide details of your nominated planning representative when submitting your registration.

Note: Providing a planner is encouraged but not mandatory for participation in the exercise.

The Participant Role

The participant role requires a strong understanding of your organisation's cyber incident response and crisis management arrangements, enabling meaningful contribution throughout the exercise. Participants should reflect those individuals who would be actively involved in responding to a live cyber incident.

The exercise scenario is designed to explore a range of potential responses rather than arrive at a single solution. Participants will be encouraged to share insights, consider different approaches, and collectively examine how the ecosystem may respond under varying conditions.

Participants are also encouraged to propose innovative and alternative approaches to the challenges presented during the exercise. Discussions are intended to be exploratory in nature and do not represent formal or endorsed positions. The objective is to foster a collaborative environment where diverse perspectives support a deeper understanding of potential response strategies.

Commitment

Planners will be required to commit to a series of planning meetings to develop and agree on the exercise aim and objectives, design the scenario and injects, and prepare supporting documentation to ensure the successful delivery of the exercise.

Activity	Date	Time
Kick off meeting	27 May 2026	10am-12pm
Planning meeting 1	3 June 2026	tbc
Planning Meeting 2	24 June 2026	10am-12pm
Planning Meeting 3	15 July 2026	10am-12pm
Planning Meeting 4	5 Aug 2026	10am-12pm
Exercise	**19 Aug 2026**	**9:15am-4pm**

Planners will also be required to review draft materials and provide feedback between meetings as needed. They are welcome, and encouraged, to attend the exercise as observers.

Participants are expected to prepare for and attend the exercise in person on 19 August. The exercise will be held in Melbourne, with arrival between 9:00am and 9:15am (AEST), and activities scheduled to conclude at approximately 4:00pm (AEST).

Cost and Risks

There is no registration fee for participation. Participating organisations will be responsible for their own costs and for managing any associated risks.

Governance

Michelle Bower, Chief Executive Officer of GNGB, will serve as Exercise Director, overseeing the delivery of the cyber security discussion exercise. She will be supported by the Exercise Planning Group, with regular reporting provided to the GNGB Board of Directors.

Location

The exercise will be conducted in person at a venue in Melbourne, to be confirmed.

Planning meetings will be held virtually via Microsoft Teams in the lead up to the exercise. The initial planning meeting may be conducted in person, subject to confirmation.

Evaluation

The exercise evaluation will be developed by the Exercise Planning Group through the collection of observations and insights gathered during the exercise, as well as participant responses to digital questions posed throughout. Responses will be anonymised to ensure organisations and individuals are not identifiable.

These will be compiled into an After Action Report, which will be shared with participating organisations. A summary report may also be shared more broadly with stakeholders.

Registration

Registrations are requested by **1 May.**

Points of Contact

Ms Michelle Bower, CEO, GNGB
michelle.bower@gngb.com.au

Ms Mary Costello, Operations Support Manager, GNGB
mary.costello@gngb.com.au