Australian Government
National Office of Cyber Security

National Office of Cyber Security
Cyber Security Preparedness Exercises

The National Cyber Security Coordinator (the Coordinator), supported by the National Office of Cyber Security (NOCS), drives forward the necessary work to ensure Australia is best positioned to respond to the opportunities and threats of the digital age.

Vision, Mission and Values

The Coordinator's vision is for the NOCS to be trusted by Australians to deliver coordinated cyber preparedness, response and recovery for a cyber conscious and secure Australia. The NOCS's mission is to enable, and support trusted and efficient partnerships to improve national cyber preparedness and to coordinate major cyber incident responses.

Both the vision and mission are guided by the NOCS's values of empowerment, championing effective outcomes, collaborating to deliver the best outcomes for our stakeholders, demonstrating excellence in our work, communicating and engaging with clear intent and clarity, and building connectivity and trust across industry and the Australian Government.

Exercise Philosophy

Cyber security preparedness exercises are crucial because they test and refine incident response plans, ensuring a coordinated and effective response during a real cyber incident. They build muscle memory, improve decision-making, foster better team collaboration across organisations, help meet regulatory compliance, enhance reputation, and can ultimately reduce the overall financial impact and downtime of a breach.

In line with the NOCS's vision, mission and values the **NOCS Exercise Philosophy** centres on a structured approach to practice, validate and refine our collective ability to respond to cyber incidents by simulating real-world scenarios in a controlled, low-risk and trusted environment. Key elements include a focus on improving decision-making and communications, fostering a zero-blame culture for open discussion, and a commitment to continuous improvement by documenting lessons learnt to enhance preparedness and resilience in an increasingly complex threat environment.

The NOCS Exercise Philosphy is underpinned by the following **PREPARE** principles:

Partnerships – Build strong partnerships, understand roles and responsibilities, and emphasise collaboration before an incident.

Realistic Simulations – Use plausible, realistic scenarios tailored to the industry sector's specific threat landscape and business context.

Establish Communications – Establish clear communication strategies to ensure timely information sharing during incidents.

Practice and Validate – Use national plans, industry frameworks, incident response plans, procedures, and capabilities.

Achieve objectives – Design exercises with specific objectives for participants and other interested stakeholders

Risk-based Approach – Prioritise and conduct exercises to identify and understand risks.

Evaluate and Improve – Ensure ongoing improvement, where lessons learnt are documented and integrated into processes.

What is Consequence Management?

The NOCS helps government and industry work together to identify and mitigate the secondary harms that may result from a cyber security incident. In the most severe instances, this could include 'real world' impacts. This may require the activation of emergency management arrangements, such as the National Coordination Mechanism.

The aim of consequence management is to predict, identify, and manage the social, economic, and environmental repercussions of a cyber security incident. The purpose is to mitigate harm and promote a quick recovery.

Coordination and Consequence Management Exercises

The NOCS' cyber security preparedness activities are primarily delivered to government and industry entities through coordination and consequence management exercises. Coordination and consequence management exercises practice the decision-making response to a cyber security incident. This is in contrast to other exercises, such as technical exercises, which are focused on testing an entity's technical capabilities to respond to cyber incidents.

NOCS exercises help ensure internal cyber security and crisis response arrangements are integrated, practiced and understood internally. Additionally, the exercise discussions help entities understand the role of government, the protocols for government engagement, and the options for assistance. Exercises are critical tools for uplifting cyber security preparedness before an incident occurs by ensuring that all crisis coordination processes are considered.

Exercise Programs

The NOCS has responsibility for supporting government, critical infrastructure and the broader economy to prepare for major cyber incidents.

National Cyber Exercise Program (NCEP)

The National Cyber Exercise Program (NCEP) is a key measure under Shield 4 of the *2023-2030 Australian Cyber Security Strategy*. Through the NCEP, the NOCS works with Australian Government agencies to establish a combined list of all completed and planned Commonwealth cyber security exercises.

The NCEP enables the Coordinator to oversee the Australian Government's cyber security preparedness efforts. The NCEP aids the Coordinator and the NOCS in identifying any gaps or sectors in the program that require further focus. Through collating these exercises, the NCEP will enable all participating Australian Government agencies and entities to ensure that their respective programs are integrated for maximum impact.

NOCS Exercise Program (NOCS-EP)

NOCS exercises aim to improve government and industry collaboration, inform future coordination between the NOCS and industry stakeholders during cyber security incidents, and ensure internal plans, policies and procedures are fit for purpose.

The NOCS-EP is conducted through tabletop discussion exercises focused on improving stakeholders' understanding of the NOCS's role in coordinating the national response, consequence management, and communication activities in the event of cyber security incidents. This explains how the NOCS responds to incidents under the Australian Government Crisis Management Framework, the Australian Cyber Response Plan, and the NOCS' Sector Playbooks.

The NOCS develops, delivers, participates in and/or observes coordination and consequence management exercises across the Australian economy and government. These exercises provide an opportunity for government and industry stakeholders to collaborate in realistic, consequence driven scenarios that explore the full spectrum of incident response plans, consequence management and communication arrangements.

The NOCS-EP includes NOCS-led exercises and external exercises attended by the NOCS. Exercises designed and delivered by the NOCS seek to educate stakeholders and explore processes that would be used to coordinate the response to cyber security incidents.

There are three different types of exercises delivered by the NOCS under the NOCS-EP:

1. A Flagship Exercise is the NOCS's major exercise output that targets senior levels of government or industry stakeholders.
2. A standard NOCS Exercise targets working levels of key government and/or industry stakeholders.
3. Exercise Lite activities are targeted, short-format sessions designed around specific issues, for example, that were previously explored in another exercise or which may inform the development of a future Flagship Exercise or Exercise.

NOCS involvement in other exercises

The NOCS can deliver its objective of educating stakeholders on the NOCS's role through participating in exercises delivered by other government and industry stakeholders.

If you are interested in having the NOCS attend your exercise or would like to discuss the development of an exercise, please reach out to NOCS.Exercises@homeaffairs.gov.au.