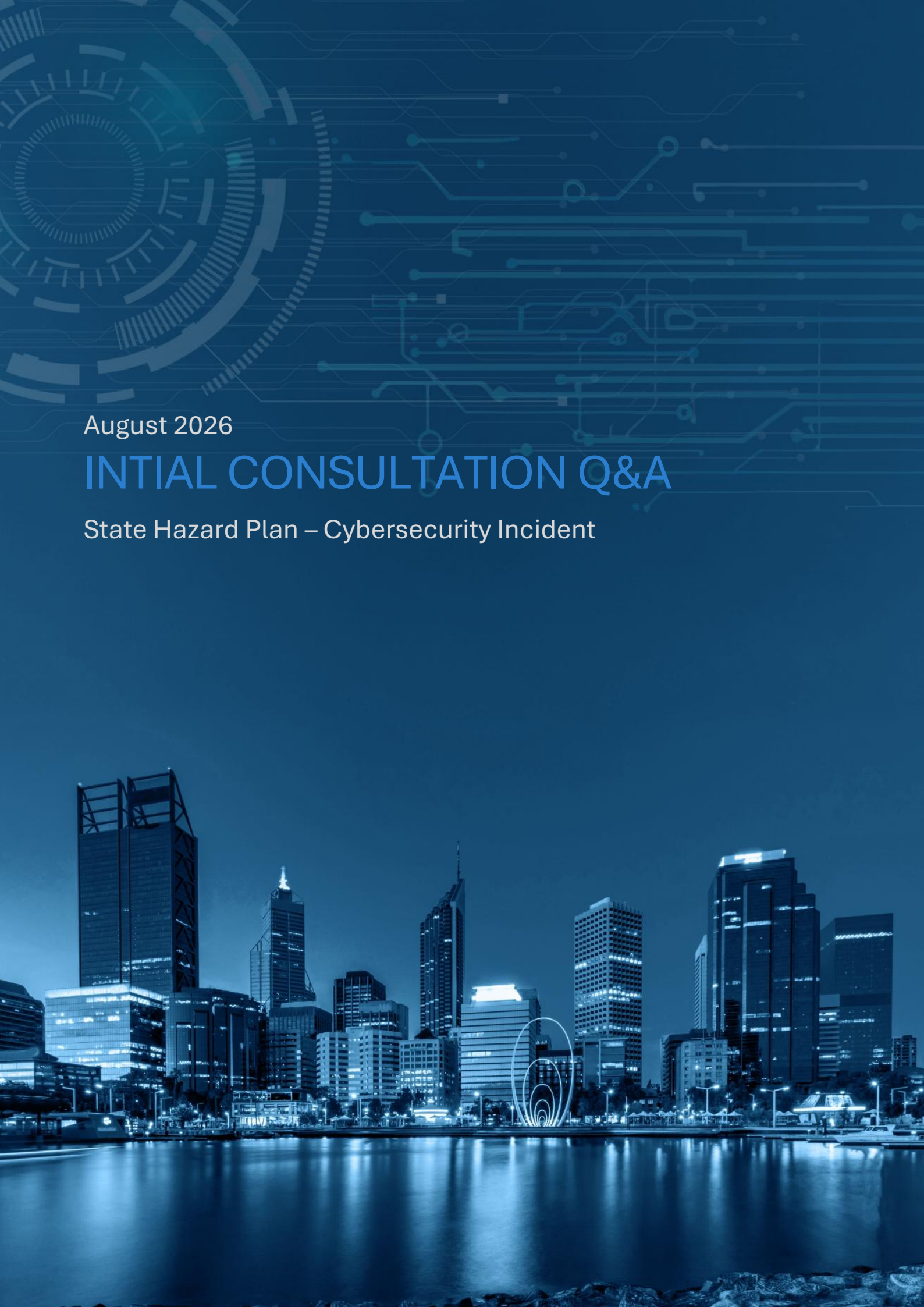




August 2026

INITIAL CONSULTATION Q&A

State Hazard Plan – Cybersecurity Incident



Introduction

The Emergency Management Regulations 2006 designates the Department of the Premier and Cabinet (DPC) as the Hazard Management Agency (HMA) for the Cybersecurity Incident Hazard. Within the DPC, the Office of Digital Government (DGov) has been preparing the State Hazard Plan – Cybersecurity Incident (SHPCI) for approval by the State Emergency Management Committee (SEMC). As part of this approval process, two rounds of consultation are required.

The initial consultation round was completed in June 2026, with the second round of broad consultation to run for 12 weeks from August 31 to November 20.

The purpose of this document is to identify key themes and their remediation from the initial consultation. This will provide organisations engaging with the final consultation with an insight into feedback previously received, to better focus new feedback on areas that are within the scope of the SHPCI and that improve the overall quality of the document.

This document provides users with:

1. A summary of the key themes of feedback from the initial consultation
2. A question-and-answer format overview of feedback, organised by the sections within the SHPCI
3. A table detailing changes to the initial draft SHPCI
4. An overview of the WA Whole-of-Government Cyber Security Incident Coordination Framework (WACSICF)



General

Feedback	Response
The six-hour reporting timeline for notifying the Office of Digital Government (DGOV) of an incident is too ambitious.	• This requirement is aligned with the upcoming revision of the WA Cyber Security Policy (WACSP). • Advancements in artificial intelligence (AI)-assisted vulnerability detection and exploitation have reduced the time until threat actors can feasibly exploit a vulnerability. This timeline will only continue to reduce as AI capabilities improve. • For DGOV to assist a WA Government Entity (WAGE) in containing/responding to a cyber incident, early notification is essential, hence the need for the reporting timeframe.
The document is missing a hyperlink to a specific document.	• Some documents referred to by the SHPCI are not intended to be distributed publicly. • Because the SHPCI is public document, hyperlinks to these documents cannot be included, examples include the WA Government Cyber Security Incident Coordination Framework (WACSICF).
The SHPCI should contain practical implementation and compliance guidance for stakeholders.	• The SHPCI is not intended to be an operational guideline, rather a description of the HMA responsibilities under the State Emergency Management arrangements. • Additional information on implementation and compliance is available in the WA Whole-of-Government Cyber Security Incident Coordination Framework (WACSICF), which outlines: ○ WA cyber security incident levels ○ WA cyber security incident escalation workflows ○ WA cyber security incident responsibility flows ○ A high-level incident response plan template ○ Guidance on the release of public information. • For WA Government Entities (WAGEs) additional guidance material is available to support the implementation of the policy. DGOV will develop additional supporting

Feedback	Response
	material where necessary to support the SHPCI, in the form of procedures, playbooks and guidelines within the State Emergency Management Framework. - The State Emergency Framework also contains guidelines and procedures for: - Emergency risk management. - Managing exercises.
Which version of the WACSP is the SHPCI aligned to?	The SHPCI aligns with the draft 2026 revision of the WACSP. It is anticipated the 2026 Policy will be released in Q4 of 2016.
Plan should focus more heavily on Operational Technology, given the focus on avoiding harm to people and the environment.	- The SHPCI provides a technology-neutral framework for the prevention and mitigation, preparedness, response and recovery (PPRR) of cyber security incidents. - The arrangements are intended to remain applicable as technologies and threat environments evolve, while allowing the circumstances and consequences of each incident to determine the appropriate response.

Part One: Introduction

Feedback	Response
Add an executive appendix covering: - Actions within the first 0-6 hours - Matrix outlining authority for decision making - Triggers for hazard declaration - Common failure points	- The SHPCI sets the strategic emergency management arrangements and is not intended to prescribe detailed operational actions of an incident. - Operational workflows should be contained within the organisational playbooks and procedures which are guided by the WACSICF the WA Government Cyber Security Policy. - Because of the wide scope of scenarios that are within the scope of a cybersecurity incident, it is difficult to conceive of failure points that are applicable across all conceivable scenarios. Identifying limitations and constraints in a public document would expose vulnerabilities and potential avenues of exploitation for threat actors.

Part Two: Prevention and Mitigation

Feedback	Response
Identify constraints where prevention may be limited or not possible.	- Identifying limitations and constraints in a public document would expose vulnerabilities and potential avenues of exploitation for threat actors. - Each entity should understand its risk profile and implement proportionate treatments to reduce the likelihood and potential consequences of a cyber security incident.

Part Three: Preparedness

Feedback	Response
Is this plan appropriate for Government Trading Enterprises (GTEs) with resources and procedures for responding to a cyber crisis?	The Plan provides the framework for HMA and cross-agency coordination where an incident requires broader or State-level emergency management arrangements. An organisations procedures should align with the relevant frameworks outlined in the plan.
Will agencies be required to update processes and documents to prepare for a state incident?	Only to the extent that any existing processes/documentation conflict with the SHPCI.
Establish minimum preparedness metrics.	Appendix C of the SHPCI has been amended to clearly outline Preparedness requirements for WAGEs.
Establish Whole-of-Government cyber exercise cadence.	- The SHPCI will be exercised in accordance with the requirements of Part 4 of the State Emergency Management Policy. - Agencies may undertake their own exercises and participate in state and federal based exercises as required.

Feedback	Response
Include additional information on preparing for activation, including: • Escalation readiness • Coordination forums	• The SHPCI establishes coordination arrangements for the response and recovery phases. Detailed activation guidance is provided in the WACSICF.
Clearly define agency preparedness expectations: • Planning activities • Readiness activities • Engagement with state level coordination arrangements	Clarification provided. Additional information and requirements are outlined in both the WACSP and the WACSICF.
Explicitly address planning for cross-agency and cross-sector dependencies. Consider including cross-agency scenario testing and dependency planning as requirements.	• The cross-sector dependencies will depend on the consequential hazards that arise from the cyber security incident. • The SHPCI has been designed to allow organisations that have HMA, combat agency and support organisation responsibilities designated by the EM Regulations to address consequential emergencies and to aid the incident controller as required. This allows the most appropriate agency to manage/exercise consequential hazards.
Clarify preparedness expectations where shared services environments exist.	• Additional information provided in Appendix C of the SHPCI, which outlines the preparedness responsibilities for WAGEs and MSPs involved in a SHPCI response.

Part Four: Response

Feedback	Response
Is this plan interoperable with existing agency response arrangements?	• Yes, however, where agency response arrangements conflict with the SHPCI, the agency will be required to align their arrangements.
To what extent is incident control granted to the HMA by the SHPCI?	• The powers available to the HMA to manage a CSI is prescribed in the EM Act, Regulations and Framework.
The SHPCI requires a technical baseline of controls, will material be developed for entities that don't currently meet that baseline during cyber incidents?	• The WA Government Cyber Security Policy sets the minimum cyber security controls for entities within its scope. • DGov provides an established uplift program to help WA Government entities strengthen these controls.
Compile reporting requirements into single table.	• Reporting requirements will differ between WAGEs, depending on whether they have obligations dictated by other legislative requirements.
There is not exact alignment between State and National incident levels, could this confuse users?	• WA organisations should use on the WA incident levels. DPC as the HMA will act as the conduit between an impacted organisations and federal agencies.
SHPCI would benefit from supplementary and preparatory information that can be used as a template, covering: • State simulation exercises • Detailed playbooks • Other response and recovery activities	• DGov provides guidance and support to help entities develop their internal processes and procedures. These resources will continue to evolve in response to the changing threat landscape and entity needs.

Feedback	Response
Should the SHPCI reference notifiable breaches under the Privacy and Responsible Information Sharing Act 2024 (PRIS Act)? How do PRIS Act notification obligations interact with reporting as required by the SHPCI?	Procedures for meeting PRIS Act notification obligations should form part of each organisation's internal cyber security incident response processes and playbooks.

Part Five: Recovery

Feedback	Response
Edited Feedback: Case studies would assist WAGEs understand resources required for incident response and potential length of recovery/response.	Noted.
Establish post-incident performance measures.	Under consideration.

Amendments following initial consultation

This section outlines changes that have been made to the SHPCI between the conclusion of the initial consultation and the beginning of the public consultation.

Section	Revisions
1.4 Roles and Responsibilities	Paragraph added outlining where coordinated emergency arrangements might be needed.
1.4.1 Operational responsibility for continuity of essential services	Paragraph added outlining operational responsibility for continuity of essential services.

Section	Revisions
2.3 Capability Assessment	• Outlines planning considerations for significant, prolonged cyber incident impacting multiple government agencies and service providers.
2.4.1 State Prevention and Mitigation Strategies	• Added information on targeted awareness programs for high-risk sectors
3.3.1 Community specific arrangements	• Section added outlining preparedness arrangements for the community.
4.1.3 Multiple Hazards	• Section revised for clarity.
4.2 Response Arrangements	• Paragraph added detailing how the nature, complexity and consequences of an incident change the required response arrangements.
4.2.2 State Level Arrangements	• Paragraph added outlining the responsibility of WAGE personnel during the response phase and the information they provide to the HMA and incident controller.
4.42 Incident Levels	• Added a paragraph on required considerations for assessing the appropriate response level and the requirement for the HMA to consider affected entity assessments.
4.4.3 Incident Management Team Structure	• Section added outlining the Incident Management Team structure for cybersecurity events.
4.4.4 Transfer of Control	• Section revised to outline which circumstances will result in a transfer of control.
4.5 Public Information and Warnings	• Added sentence that confirms the ability of entities to issue time-critical public information. • Added a list of platforms that may be used to issue public information and warnings.

Section	Revisions
4.7 Support Services	Paragraph added detailing the Department of Communities role as a support agency.
4.9 Funding Arrangements for Response	Section added outlining the funding burden arrangements for a SHPCI response.
5.1.1 Accountable Authorities	Paragraph added detailing management arrangements where an incident impacts essential services or shared service platforms.
5.2 Recovery Characteristics and Considerations	- Expanded section to outline recovery characteristics and considerations, including: - Impacts caused by the hazard; - Impacts from response measures; - Community impacts.
5.3.2 Impact Statement	- List of stakeholders engaged in the preparation of an impact statement added. - List of positions authorised to approve an impact statement added.
5.4 Transition of Recovery Coordination	List of considerations that inform the timing of transferring responsibility for recovery coordination added.
5.5.1 Transition to business-as-usual arrangements	Paragraph outlining conditions for transitioning to business-as-usual arrangements added.
Appendix C: Roles and responsibilities	- Added section outlining the purpose of the appendix. - Responsibilities now split into the phase of recovery that they exist for.

Acronyms

Term	Acronym
Artificial Intelligence	AI
Australian Cyber Security Centre	ACSC
Office of Digital Government	DGov
Cyber security	CS
Cyber Security Unit	CSU
Department of the Premier and Cabinet	DPC
Hazard Management Agency	HMA
Operational Technology	OT
Managed Service Provider	MSP
Privacy and Responsible Information Sharing Act 2024	PRIS Act
State Emergency Management Committee	SEMC
State Hazard Plan	SHP
State Hazard Plan – Cybersecurity Incident	SHPCI

Emergency Management Act 2005	EM Act
Emergency Management Regulations 2006	EM Regulations
WA Government Cyber Security Policy	WACSP
WA Government Entity	WAGE
WA Government Entities	WAGEs
Government Trading Enterprises	GTEs
National Institute of Standards and Technology	NIST
International Organization for Standardization	ISO
Cyber Incident Management Arrangements	CIMA
National Cyber Security Arrangements	NCSA
WA Security Operations Centre	WASOC
WA Whole-of-Government Cyber Security Incident Coordination Framework	WACSICF