Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Enhanced Cyber Security Obligations – Incident Response Planning

Part 2C Division 2 *Security of Critical Infrastructure Act 2018*
Guidance

Contact us

Enquiries regarding the licence and any use of this document are welcome to sons@homeaffairs.gov.au, or:

Systems of National Significance Branch,
Department of Home Affairs
PO Box 25, BELCONNEN, ACT 2616

Contents

Preface

This guidance has been prepared to assist responsible entities for Systems of National Significance to comply with the Incident Response Planning Enhanced Cyber Security Obligation as part of the *Security of Critical Infrastructure Act 2018 (SOCI Act)*.

Systems of National Significance

Systems of National Significance (SoNS) are Australia's most important critical infrastructure assets by virtue of their interdependencies across sectors and the potential for cascading consequences to other critical infrastructure assets and sectors if disrupted. The power to declare an asset a SoNS is held by the Minister for Home Affairs.

Under the SOCI Act, SoNS may be subject to one or more Enhanced Cyber Security Obligations (ECSOs). The ECSOs have been designed to give Australians confidence that critical infrastructure entities have well-tested plans in place to respond to and mitigate against a cyber attack. Over time, the ECSOs will support the sharing of near-real time threat information to provide industry and Government with a more mature understanding of emerging cyber security threats and the capability to reduce the risks of a significant cyber attack.

In addition to the ECSOs, SoNS remain subject to all obligations that applied to that critical infrastructure asset under the SOCI Act before it was declared a SoNS.

This document provides guidance to SoNS entities required to implement and comply with the Incident Response Planning obligation, to ensure that our most important critical infrastructure assets are protected from those that wish to do us harm.

Enhanced Cyber Security Obligations

The ECSOs are outlined in Part 2C of the SOCI Act. Each obligation is separate and is individually applied to an asset.

The ECSOs include:

- developing cyber security incident response plans to prepare for a cyber security incident;
- undertaking cyber security exercises to build cyber preparedness;
- undertaking vulnerability assessments to identify vulnerabilities for remediation; and
- providing system information to develop and maintain a near-real time threat picture.

What is an Incident Response Plan?

An incident response plan is a written plan that outlines how a responsible entity for a SoNS will respond to a cyber security incident. While uplifting cyber security and preventing attacks from occurring will always be the number one priority, there may be some threats that cannot be thwarted. Incident response plans provide an organisation with a clear understanding of 'what to do' and 'who to call' to minimise the impact of an incident and continue to provide services to the community.

To be effective, an incident response plan should:

- align with an organisation's emergency, crisis and business continuity arrangements, as well as jurisdictional and national cyber and emergency arrangements; and
- support personnel to fulfil their roles by outlining their responsibilities and all legal and regulatory obligations.

What is the Incident Response Planning obligation under the SOCI Act?

The Secretary of the Department of Home Affairs (or a delegate) may apply the Incident Response Planning obligation to a responsible entity for a SoNS. The obligation requires the entity to adopt, maintain and comply with an incident response plan, which must be in relation to the SoNS and cyber security incidents. The entity must also review the plan on a regular basis and take all reasonable steps to ensure the plan is up to date.

Before applying the Incident Response Planning obligation, the Secretary must consult the responsible entity and consider the costs, reasonableness and proportionality of applying the obligation, as well as any other matter that the Secretary considers relevant. This may include whether a similar or equal regulation already applies to the SoNS.

Notification

If the Incident Response Planning obligation is applied, the entity will receive written notice specifying when the obligation comes into effect – the SOCI Act ensures this will be no less than 30 days.

Once in effect, the entity must provide the Secretary with a copy of the incident response plan 'as soon as practicable' after the plan is adopted or varied.

The Incident Response Planning obligation is an enduring obligation. This means that once applied, it will remain in effect until revoked. The Secretary (or a delegate) may, by written notice, revoke the determination.

The Department's approach

The initial approach to the Incident Response Planning obligation

The Department's initial approach to implementing the Incident Response Planning obligation is to ensure a baseline incident response capability across all SoNS, and that plans are well-practised and tested. This component will be supported through the application of the Cyber Security Exercise obligation.

The Incident Response Planning obligation under the SOCI Act is focused on cyber security incidents and is not intended to address hazards more broadly. While the Department will accept incident response plans that include an all hazards approach, it must be clear that the plan has a significant focus on cyber.

Best practice incident response plans do not apply to specific cyber security incidents (although components of them may focus on specific types), but rather apply to cyber security incidents more generally. This ensures procedures are in place to address the various methodologies that may be adopted in a cyber attack.

While the SOCI Act allows for the provision of rules to be made that prescribe certain requirements for an incident response plan, the Department has not created rules at this time. The Department acknowledges that responsible entities are best placed to construct their incident response plan, taking into account a variety of factors including the services provided by the asset, the extent and nature of interdependencies, and the threat environment.

If a cyber security incident has had a relevant impact on a SoNS, the Department will work closely with the entity to ensure it has complied with its Incident Response Planning obligations. As part of this process, the Department may request additional information on a voluntary basis or, if necessary, the Secretary may issue a notice requiring information or documents from the entity in accordance with section 37 of the SOCI Act.

The Department's approach to regulatory compliance

The Cyber and Infrastructure Security Centre's Compliance and Enforcement Strategy (April 2022) outlines the Department's regulatory principles and approach.

In applying the Enhanced Cyber Security Obligations, our focus is on education and engagement with SoNS responsible entities, and ensuring all SoNS have in place well-tested plans for responding to cyber security incidents that could have a relevant impact on their systems.

Key points

- Incident response plans must be in relation to the responsible entity's SoNS asset or assets, and outline how the entity would respond to cyber security incidents that could have a relevant impact on their systems.
- If an entity has an existing plan that meets the above criteria, they will not need to develop a new or separate plan for the purpose of meeting this obligation.
- Responsible entities are best placed to design and structure an incident response plan that works for their unique corporate structure and operational requirements.
- Incident response plans may be one document or multiple documents.
- If an incident response plan is a single document but refers to other organisational documents, the entity is encouraged to provide those documents to the Department as part of their incident response plan package.
- An incident response plan may relate to one or more SoNS assets. It may include both SoNS and non-SoNS assets.
- The Department can make rules that specify certain requirements that an incident response plan must include. No rules have been made at this time.
- Responsible entities are required to review their incident response plans on a regular basis. Entities are encouraged to do so against the 'What Good Looks Like' guidance framework (see pages 11 – 20) to determine whether their plan is fit for purpose or requires updating.

Applying the obligation
What to expect: a step-by-step guide

The process to apply the Incident Response Planning obligation is similar to the SoNS declaration process, as the responsible entity must be consulted prior to the obligation being switched on. A key difference is that the power to declare an asset a SoNS is held by the Minister, whereas the power to apply any one of the ECSOs is held by the Secretary (or a delegate).

1 Consultation

Responsible entities will receive written notification from the Department advising that the Secretary (or a delegate) is considering applying the Incident Response Planning obligation. This letter commences the consultation process and invites entities to provide a written submission. The Department will also consult any relevant Commonwealth regulators with functions relating to the security of the SoNS. During consultation, the Secretary will consider the costs, reasonableness and proportionality of applying the obligation.

Consultation timeframe – there is no minimum timeframe for consultation under this provision within the SOCI Act. The Department will specify the timeframe in the consultation letter.

Consultation form – this will consist of town hall-style information sessions and one-on-one meetings. Entities can choose to provide a written submission.

2 The obligation is applied

Following consultation, the responsible entity will receive written notice from the Secretary (or a delegate) advising whether or not the obligation has been applied. If the Secretary decides to apply the obligation, the written notice will specify when the obligation comes into effect.

Timeframe – the SOCI Act ensures that responsible entities will have at least 30 days from the date the notice is provided before the Incident Response Planning obligation comes into effect. This timeframe is for an entity to have an incident response plan in place.

3 Provide plan to the Secretary

The responsible entity must provide a copy of the incident response plan to the Department 'as soon as practicable after adoption'. This may include a single document, or if the plan consists of multiple documents, all relevant documents. Documents can be provided via the secure document portal.

Timeframe – what is 'practicable' will vary on a case-by-case basis. The Department will work with entities during consultation and once the obligation has been applied to agree to an appropriate timeframe.

4 Review and Update

Responsible entities must review their incident response plan on a regular basis and must take all reasonable steps to ensure the plan is up-to-date. If the plan is varied, the entity must provide the varied plan to the Secretary.

Regular review – while this is not defined under the SOCI Act, the Department recommends that entities review their incident response plan at least once a year. Entities may choose to do this following a cyber security exercise which tests their incident response arrangements.

When to provide a varied plan to the Department – entities should provide a varied plan to the Department if material changes have been made. This would not include superficial updates. Examples of a material change may include: the addition or removal of information relating to decision-making during an incident, or an update to roles and responsibilities. Entities are encouraged to discuss any changes with the Department prior to submitting an updated version.

Protecting sensitive information

What documentation do responsible entities need to provide?

The Department acknowledges that evidence for meeting the Incident Response Planning obligation is likely to be found across a variety of supporting documents.

If not contained within the incident response plan directly, the following types of documents may be referenced within the incident response plan and could be provided as supporting documents:

- incident response playbooks or procedures;
- crisis management or recovery procedures;
- risk management documents;
- information, technology, and cyber security policy documents;
- threat or risk assessments; or
- asset identification and classification framework.

Templates

There is no requirement to use a specific template. The Australian Signals Directorate offers a number of useful resources, including a cyber incident response template.

What will the Department do with an entity's incident response plan?

The Department will review incident response plans to:

- determine whether it meets the requirements outlined in section 30CJ of the SOCI Act;
- understand the cyber security incident response capability of SoNS responsible entities and across the SoNS cohort as a whole;
- identify opportunities to support the uplift of the cyber security incident response capabilities of SoNS responsible entities, including through the development of best practice guidance; and
- determine if any rules are required to uplift the cyber security incident response capabilities of an entity, a sector or all SoNS.

How safe is the entity's information submitted via the secure portal?

Entities should provide their incident response plan and any supporting documents via the Department's secure document portal.

The secure portal has been developed to ensure that sensitive information provided for the purpose of meeting obligations under the SOCI Act, such as incident response plans and related documents, is immediately safe-dropped from the website link to a classified systems location.

Thereafter, multiple layers of security protect the data. It is stored on the Department's SECRET system and within a restricted portal created solely for the purpose of storing information relating to the Enhanced Cyber Security Obligations.

Government employees with a minimum Negative Vetting 1 security clearance require a business need-to-know in order to access this information. This information must be handled carefully in accordance with the SECRET classification of the system, the protected information provisions under the SOCI Act, as well as with integrity and professional standards frameworks.

The Department's SECRET network and the Enhanced Cyber Security Obligations portal is managed by appropriately cleared Departmental staff. No third parties have access to the portal.

More broadly, we operate under the Protective Security Policy Framework (PSPF) which ensures that all information created, stored, processed, or transmitted in or over government information and communication technology systems is properly managed and protected throughout all phases of a systems life cycle.

Incident Response Planning – What Good Looks Like

The below framework provides guidance to entities developing, reviewing and updating a cyber security incident response plan.

Overview

- Responsible entities are best placed to construct their incident response plan, taking into account a variety of factors including the services provided by the asset, the extent and nature of interdependencies, and the threat environment.
- To support entities in setting out an incident response plan that outlines the processes and procedures to prepare for and respond to a cyber security incident, the Department has developed the following framework which considers eight key criteria.
- The Australian Signals Directorate also has a number of useful resources, including cyber incident response guidance, templates and checklists.

Purpose of this section

It is important to note that this framework is not mandatory. It has been developed to support entities with their approach to continual incident response improvement.

The Criteria

Criterion code	Criterion name
IR.1	Alignment to cyber security posture and risk management program as applicable
IR.2	Identify most likely incident scenarios (e.g. accidental, malicious disruptions)
IR.3	Identify detection/first assessment capabilities
IR.4	Identify investigation and remediation procedures
IR.5	Identify decision and escalation points
IR.6	Communications management
IR.7	Roles and responsibilities
IR.8	Post incident review/lessons learned
Criticality	Each criteria includes sub criteria which has been designated a level of criticality: critical, high and medium. This criteria can be used to assist entities to prioritise certain components when developing and reviewing an incident response plan.

Criterion IR.1: Alignment to cyber security posture and risk management policy

Outcome

A best practice incident response plan (IRP) should be aligned to the responsible entity's broader risk management policies. This will ensure that the IRP considers the most likely attack scenarios and the most business-critical assets to defend.

An effective IRP will identify the threat vectors and threat actors that are most likely to cause a serious cyber security incident that will impact a particular SoNS. Identifying the most likely tactics, techniques and procedures that will be used against a SoNS will allow defenders to prepare an IRP that is most appropriate to respond to the most likely and/or most impactful cyber attack scenarios.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP cover all the relevant regulated systems? **(Critical)**	The IRP contains appropriate procedures for all relevant regulated systems.	The IRP contains appropriate procedures for the majority of relevant regulated systems.	The IRP does not contain procedures for all relevant regulated systems.
Do the business-critical assets in the IRP align with the SoNS risk management policies? **(High)**	The IRP considers all relevant critical components of assets that are identified in the SoNS risk management policies. The IRP describes this alignment.	The IRP contains most of the relevant critical components of assets that are identified in the SoNS risk management policies. The IRP partially describes this alignment.	The IRP does not contain or is missing most of the relevant critical components of assets that are identified in the SoNS risk management policies. The IRP does not describe this alignment.
Does the IRP include Standard Operating Procedures that address the likely risks as stated in risk management policies? **(High)**	The IRP contains all relevant Standard Operating Procedures that address likely risks that are identified in the SoNS risk management policies. The IRP describes this alignment.	The IRP contains some of the relevant Standard Operating Procedures that address likely risks that are identified in the SoNS risk management policies. The IRP partially describes this alignment.	The IRP does not contain or is missing the majority of the relevant Standard Operating Procedures that address likely risks that are identified in the SoNS risk management policies. The IRP does not describe this alignment.
Does the IRP align to wider cyber security strategy and outcomes? **(High)**	The IRP aligns to the SoNS' strategic cyber security strategy or uplift outcomes. The IRP describes this alignment.	The IRP partially aligns to the SoNS' strategic cyber security strategy or uplift outcomes. The IRP partially describes this alignment.	The IRP does not align to the SoNS' strategic cyber security strategy or uplift outcomes. OR The IRP does not describe the alignment of the cyber security strategy and outcomes.

Criterion IR.2: Identify most likely incident scenarios (e.g. accidental, malicious disruptions)

Outcome

Best practice IRPs do not apply to specific cyber security incidents (although components of them may focus on specific types), but rather apply to cyber security incidents generally. This ensures procedures are in place to address the various methodologies that may be adopted in any cyber-attack. However, an entity should also identify scenarios that are most likely to affect SoNS.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP consider threat actors and incident scenarios? ***(High)***	The IRP considers all likely threat actors and incident scenarios to the SoNS.	The IRP includes some likely threat actors and incident scenarios to the SoNS.	The IRP includes no likely threat actors or incident scenarios to the SoNS.
Does the IRP include impact assessments for incident scenarios? ***(High)***	The IRP has included impact assessments for all likely incident scenarios identified in the responsible entity's risk management policies. These assessments include measurable metrics.	The IRP includes guidelines to conduct impact assessments against the most likely incident scenarios. These guidelines include measurable metrics.	No impact assessment information has been included in the IRP.

Criterion IR.3: Identify detection/first assessment capabilities

Outcome

Some threat actors can remain hidden on a victim's network for months or years, undertaking malicious activities without detection. This could include threat actors that are external to the system, or internal within the system, such as a malicious insider. A responsible entity's capability to detect potential cyber security incidents is a critical precursor to their IRPs.

The responsible entity should ensure it has adequate incident identification capabilities to trigger their IRP when necessary. These may be automated or human-directed capabilities. The IRP should include regular identification activities and outline the steps taken to trigger the IRP when a possible incident has been identified.

This criterion could be measured via Mean-Time-to-Acknowledge (MTTA).

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP describe adequate identification capabilities to detect cyber security incidents? ***(Critical)***	The IRP has a defined section for identification and detection of cyber security incidents. This includes standard procedures for attack identification and detection.	The IRP includes a section outlining identification and detection capabilities.	The IRP does not identify initial identification methods.
Does the responsible entity identify logging capabilities for data sources? ***(Critical)***	The responsible entity retains logs in line with the Australian Cyber Security Centre Essential 8 (Maturity 2) requirements. The responsible entity identifies logging capabilities that includes all of the following factors:	The responsible entity somewhat retains logs in line with the Australian Cyber Security Centre Essential 8 (Maturity 2) requirements. The responsible entity identifies logging capabilities that includes	The responsible entity does not retain logs in line with the Australian Cyber Security Centre Essential 8 (Maturity 2) requirements. The responsible entity identifies logging capabilities that includes

Consideration	Well Implemented	Partially Implemented	Not Apparent
	• Details of event logged (date, time, user, etc) • Logging facility used • Event log monitoring procedure • Log retention requirements.	threat least half of the following factors: • Details of event logged (date, time, user, etc) • Logging facility used • Event log monitoring procedure • Log retention requirements.	less than half of the following factors: • Details of event logged (date, time, user, etc) • Logging facility used • Event log monitoring procedure • Log retention requirements.
Does the responsible entity have a cyber security incident register prepared for when a malicious event is detected? ***(Critical)***	The responsible entity includes a template of a cyber security register that includes all the following factors: • A description of the incident • Who reported the incident (name, department, phone, email) • Who it was reported to • The date/time (When occurred, discovered, reported, began working on, resolved) • The incident type (phishing, etc) • The affected systems • The indicators of compromise • The impact to SoNS asset • The resolution.	The responsible entity includes a template of a cyber security register that includes at least half of the following factors: • A description of the incident • Who reported the incident (name, department, phone, email) • Who it was reported to • The date/time (When occurred, discovered, reported, began working on, resolved) • The incident type (phishing, malware, etc) • The affected systems • The indicators of compromise • The impact to SoNS asset • The resolution.	The responsible entity does not include a template of a cyber security register, or contains less than half of the following factors: • A description of the incident • Who reported the incident (name, department, phone, email) • Who it was reported to • The date/time (When occurred, discovered, reported, began working on, resolved) • The incident type (phishing, malware, etc) • The affected systems • The indicators of compromise • The impact to SoNS asset • The resolution.
Does the responsible entity provide evidence of monitoring with real-time alerts? (***High***)	The responsible entity has implemented two methods of monitoring for malicious activity: • Automated (e.g. sensors) • Human-directed (e.g. regular manual scans).	The responsible entity has implemented one method of monitoring for malicious activity: • Automated (e.g. sensors) • Human-directed (e.g. regular manual scans).	The responsible entity has not implemented any methods of monitoring for malicious activity.
Does the responsible entity include guidance on measuring and reporting a Mean-Time-To- Acknowledge (MTTA)? ***(Medium)***	The responsible entity includes guidance on calculating and reporting an MTTA.	The responsible entity includes guidance on reporting an MTTA.	The responsible entity does not include guidance on calculating or reporting an MTTA.
Does the responsible entity have threat hunting capabilities to identify unknown threats that may not be identified using their prevention and detection controls? ***(Medium)***	The responsible entity has documented procedures for threat hunting, including reporting requirements The IRP describes the escalation process if a possible threat is identified.	The responsible entity has incomplete or ineffective threat-hunting procedures. *OR* The responsible entity does not include reporting requirements in threat-hunting procedures. The IRP describes an ineffective or incomplete escalation process if a possible threat is identified.	The responsible entity does not have threat hunting procedures. *AND/OR* There is no documented escalation process.

Criterion IR.4: Identify investigation and remediation procedures

Outcome

Once an incident has been identified, a good IRP details the initial steps that should be taken to investigate the nature and extent of the incident. The IRP may also detail the remediation capabilities and activities that a responsible entity would undertake if systems were affected.

An effective IRP outlines what activities should be undertaken in response to specific developments in the ongoing cyber incident. This would ensure that defenders are responding to developments in the most efficient and effective manner possible. These steps should be detailed enough that defenders can simply follow the instructions as they are written. Incomplete or unclear IRP instructions will cause confusion and degrade the defender's response during an incident.

The IRP will not only be used by cyber security staff in the event of a cyber security incident. The IRP will include or link to procedures for system restoration and the mitigation of system outages. Given the detail required for such procedures, it is likely that these procedures will be separate technical documents.

IRPs will not necessarily provide complete coverage of longer term final resolution activity nor follow-up remediation work which may be required to remove malicious actors from a network. A responsible entity should contemplate, to the extent possible, potential remediation and prevention activity in the aftermath of an incident. The Department may engage with entities regarding how they address these considerations in their IRPs and provide further advice if necessary.

The responsible entity's IRP should ensure that it has relevant activities for its own circumstances. However, as a baseline, entities' IRPs should include actions for ensuring the physical safety of the responsible entity's staff and others, maximise service uptime during and immediately following the incident, and outline post-incident actions to ensure system security and prevent future incidents.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP provide procedures to ensure the availability of SoNS' systems and/or mitigate immediate service outages? ***(Critical)***	All critical components of the SoNS asset(s) have been identified and addressed within the Risk Register (or similar), and have a procedure for outage mitigation in place, including system segregation and shut-down where possible. *AND* Guidance for locating further information for all system availability procedures is supplied in the IRP.	More than 50% of the critical components of the SoNS asset(s) have been identified and addressed within the Risk Register (or similar), and have a procedure for outage mitigation in place. *AND* System availability procedures are mentioned in the IRP and cover all SoNS.	Less than 50% of the critical components of the SoNS asset(s) have been identified and addressed within the Risk Register (or similar), and have a procedure for outage mitigation in place. *AND* System availability procedures are not mentioned in the IRP.
Does the IRP contain high-level procedures to investigate the cause and methodology of the cyber security incident? ***(Critical)***	The IRP outlines all high-level requirements for investigation during a cyber security incident, including: • Assignment of responsibility to a team for investigation • Allocation of time specifically to investigate and gather evidence • An escalation point to an external Incident Response provider if necessary • Reporting requirements for results of the investigation.	The IRP contains a high-level inclusion of investigative action requirements within the cyber security incident response phases, including: • Assignment of responsibility to a team for investigation • Allocation of time specifically to investigate and gather evidence • An escalation point to an external Incident Response provider if necessary • Reporting requirements for results of the investigation.	Investigate actions are not outlined in the IRP. Reporting of investigative results is not required in the IRP.

Consideration	Well Implemented	Partially Implemented	Not Apparent
	The IRP outlines specific reporting requirements for the investigative results.	The IRP identifies the requirement for reporting investigative results.	
Does the IRP provide procedures to ensure the safety of staff and others during a significant cyber incident? ***(High)***	The IRP identifies the most likely risks to safety that could occur due to a significant cyber incident. The IRP provides information to mitigate these risks during a cyber incident. *AND* The IRP provides guidance on where to find further information on physical safety procedures during a cyber or non-cyber incident.	The IRP identifies possible risks to safety that could occur due to a significant cyber incident. The IRP provides information on how to mitigate these risks during a cyber incident. *OR* The IRP provides guidance on where to find information on physical safety procedures during a cyber or non-cyber incident.	The IRP does not provide information on procedures regarding the safety of employees or others, which could result from a significant cyber security incident.
Does the IRP contain high-level procedures to remove attacker access? ***(High)***	The IRP contains procedures for removing attacker access to SoNS' systems. The IRP also contains procedures for ensuring perimeter security and validating that the attacker's access has been removed.	The IRP contains procedures for removing attacker access to SoNS' systems.	The IRP does not contain procedures for removing attacker access to SoNS' systems.
Does the IRP contain high-level procedures regarding the collection of digital forensics and evidence? ***(High)***	The IRP contains detailed procedures for the collection of digital forensics and evidence. The procedures may involve activities by internal employees, external employees, or a mixture of the two. If the procedures involve external parties, the IRP contains contact details and guidance for the external parties.	The IRP contains some procedures for the collection of digital forensics and evidence. If the procedures involve external parties, the IRP identifies the external incident response team but does not contain contact details and/or guidance for the external parties.	The IRP does not contain procedures for the collection of digital forensics and evidence.
Does the IRP identify the communication channels that the responders will use? ***(Medium)***	The IRP identifies the primary communications channel and access details that the IRP participants are expected to use in the event of a cyber incident. The IRP also identifies at least one backup communications channel in the event that the primary communications channel is unavailable.	The IRP identifies the primary communications channel and a backup communications channel that the IRP participants are expected to use in the event of a cyber incident.	The IRP does not identify a communications channel or a backup communications channel for use in the event of a cyber incident.

Criterion IR.5: Identify decision and escalation points

Outcome

A key aspect of responding to cyber security incidents is ensuring that key decisions are made by *appropriate decision-makers in a timely manner. A good IRP describes key escalation points and* their triggers.

These escalation points can include escalation internally within the organisation, such as when managers need to be informed or when certain teams need to become involved.

The IRP must provide for mandatory cyber incident reporting as required under the SOCI Act. This should include escalation points and their triggers which then require the responsible entity to notify the Australian Cyber Security Centre (ACSC).

Escalation points and their triggers should also be identified for when responsible entities need to notify other regulatory bodies such as the Office of the Australian Information Commissioner (OAIC).

The IRP should include contact details for both internal and external escalation points, reviewed and updated regularly.

The Department strongly encourages all critical infrastructure asset owners to voluntarily report cyber security incidents to the ACSC, even if the threshold for mandatory reporting is not met.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP identify key escalation/significant decision points? ***(Critical)***	All key internal and external escalation points are identified and highlighted in the IRP. *AND* Significant decision points are identified and defined in the IRP.	Some key internal and external escalation points are identified in the IRP. *AND* Significant decision points are identified in the IRP.	Key internal and escalation points are not identified in the IRP. *AND* Significant decision points are not identified in the IRP.
Does the IRP identify the key decision maker at each escalation point? ***(Critical)***	Every escalation point in the IRP has an appointed decision maker, which are identified by their role within the organisation.	Most escalation points in the IRP have an identified decision maker.	No decision makers are identified at escalation points in the IRP.
Does the IRP identify the threshold for escalating the incident response procedures? ***(High)***	The IRP clearly identifies the thresholds for when incidents should be escalated or shared with additional internal/external teams. The IRP uses clear metrics to identify these escalation points.	The IRP identifies most thresholds for when incidents should be escalated or shared with additional internal/external teams.	The IRP does not adequately identify the thresholds for when incidents should be escalated or shared with additional internal/external teams.
Does the IRP identify the other stakeholders for each escalation point? ***(Medium)***	The IRP identifies all the stakeholders who need to be consulted or involved in each escalation point. This includes a backup decision maker in the event that the main decision maker is unavailable during the incident.	The IRP identifies some of the stakeholders who need to be consulted or involved at each escalation point.	The IRP does not identify stakeholders for consultation at each escalation point.

Criterion IR. 6: Communications Management

Outcome

Cyber security incidents are fast-paced events that evolve unpredictably. Clear and concise communication to internal and external stakeholders is important to ensure maximum effectiveness of the responsible entity's incident response. Coordinating internal communication is key to responding to the cyber incident and ensures the responsible entity maximises its cyber security capability.

Serious incidents may have financial implications as well as other implications for wider society. Communicating these implications to potentially impacted external stakeholders is an important means to mitigate negative impacts and is therefore an important aspect of a highly effective IRP.

To ensure that consistent messaging is communicated to all relevant stakeholders, the communications management section of the IRP may include who is authorised to speak on what issues, the contact details of relevant stakeholders (such as particular journalists), and draft statements that can be used for communication regarding a variety of different incidents.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP contain a communications management plan? ***(Critical)***	The IRP contains a detailed communications management plan that includes: • Internal entities that may require communication • External entities that may require communication • What information may require communication • Regulatory requirements for communications • When communications with each identified responsible entity need to be performed • How different information should be communicated • Confidence thresholds for communication with external entities.	The IRP contains a communications plan that includes at least the first four factors: • Internal entities that may require communication • External entities that may require communication • What information may require communication • Regulatory requirements for communications • When communications with each identified responsible entity need to be performed • How different information should be communicated • Confidence thresholds for communication with external entities.	The IRP does not contain a communications plan that includes the entities to be communicated with and the contents of the communication, OR does not cover the first four factors: • Internal entities that may require communication • External entities that may require communication • What information may require communication • Regulatory requirements for communications • When communications with each identified responsible entity need to be performed • How different information should be communicated • Confidence thresholds for communication with external entities.
Does the communications plan consider both internal and external stakeholders? ***(High)***	The communications plan considers most stakeholders, including: • Internal stakeholders • External stakeholders • Regulators • Government entities • Investors/financial partners • Supply chain partners • Customers/clients.	The communications plan considers less than 50% of stakeholders, including: • Internal stakeholders • External stakeholders • Regulators • Government entities • Investors/financial partners • Supply chain partners • Customers/clients.	The communications plan does not consider stakeholders or considers either internal or external stakeholders, but not both.
Does the IRP contain template talking points/media releases? ***(Medium)***	The IRP contains all of the following: • Draft talking points for serious cyber security incidents • Draft media releases for serious cyber security incidents • Templates for communicating with regulatory entities, alongside reporting requirements and guidance • Template for information sharing/reporting with the ACSC • Draft communication to employees / contractors updating them on the situation and outlining the organisation's rules around communicating with the media.	The IRP contains some of the following: • Draft talking points for serious cyber security incidents • Draft media releases for serious cyber security incidents • Templates for communicating with regulatory entities, alongside reporting requirements and guidance • Draft communication to employees / contractors updating them on the situation and outlining the organisation's rules around communicating with the media.	The IRP does not contain any of the following • Draft talking points for serious cyber security incidents • Draft media releases for serious cyber security incidents • Templates for communicating with regulatory entities, alongside reporting requirements and guidance • Draft communication to employees / contractors updating them on the situation and outlining the organisation's rules around communicating with the media.

Criterion IR.7: Roles and responsibilities

Outcome

Outlining the roles and responsibilities within an IRP ensures an efficient response to a potential cyber security incident.

Personnel should be aware of their specific roles and responsibilities within the implementation of an IRP.

This can be achieved through outlining who is responsible for what actions when a cyber security incident occurs, as well as ensuring individuals are trained at the appropriate level of detail required as per their role description.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP contain detailed division of responsibilities based on roles? ***(Critical)***	The IRP contains a detailed division of all responsibilities based on organisational roles, (rather than by individuals). The IRP allocates responsibilities to backup roles in the event that the responsible primary role is unavailable during the incident. Contact details listed in the instructions are provided for all identified positions with roles or responsibilities, including backup positions.	The IRP contains a division of most key responsibilities based on organisational roles, as well as some backup roles. Contact details listed in the instructions are outlined for all identified positions with roles or responsibilities, including backup positions, but are incomplete.	The IRP contains a division of some responsibilities based on organisational roles or individuals within the organisation. Insufficient or no contact details are identified in the IRP.
Does the IRP contain specific run sheets for specific roles? ***(Medium)***	The IRP contains run sheets or summaries for each role identified in the IRP.	The IRP contains run sheets or summaries for key IRP roles.	The IRP does not contain individual run sheets or summaries for IRP roles.

Criterion IR.8: Post incident review/lessons learned

Outcome

After an incident has been resolved, responsible entities may have an identified set of actions to ensure that an effective post-incident review is undertaken. As with all aspects of an IRP, standardising the steps of a post-incident review will ensure consistency for the organisation, regardless of staff or structural changes.

A highly effective incident review process should include identification of the vulnerability/technique used for initial entry, vulnerabilities/techniques used for lateral movement, impact(s) the incident had, the incident response process, and how to better address all these issues in future.

This process may include a calculation of costs and Mean Time to Recover (MTTR).

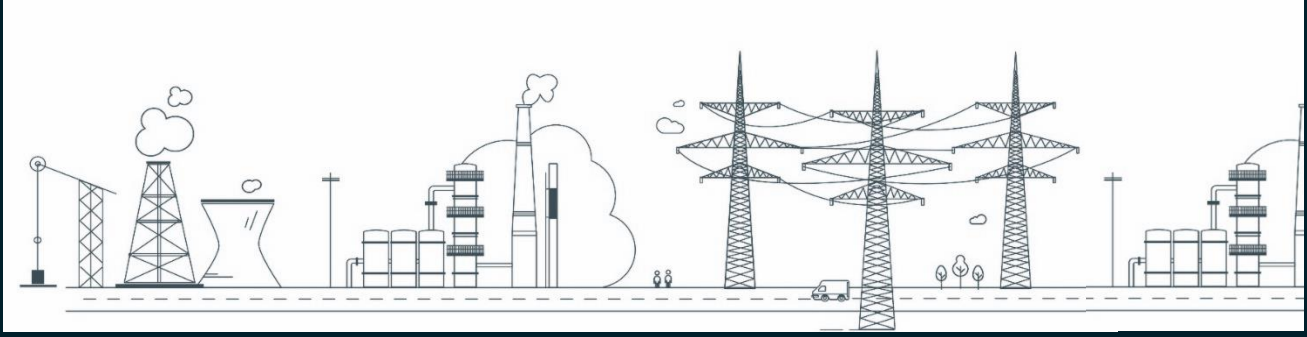
Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the IRP contain guidance on post-incident review activities? ***(Critical)***	The IRP contains detailed guidance on post-incident review activities. This guidance includes: • Actions to take after an incident is resolved • When each action is to be taken • How to complete each action listed • Reporting methods for information gathered during an incident • Guidance on implementation of critical findings following an incident.	The IRP contains some guidance on post-incident review activities. This guidance includes at least half of the following: • Actions to take after an incident is resolved • When each action is to be taken • How to complete each action listed • Reporting methods for information gathered during an incident • Guidance on implementation of critical findings following an incident.	The IRP does not contain guidance on post-incident review activities. *AND/OR* The guidance provided does not provide sufficient detail to be considered 'partially implemented.'
Does the IRP contain guidance on how to report the lessons learned to relevant stakeholders? ***(High)***	The IRP contains detailed guidance on the reporting of lessons learned, including at least: • Reporting instructions for lessons learned to stakeholders as outlined by the roles and responsibilities during an incident • A defined breakdown of the information that should be reported to stakeholders • Contact information for all relevant stakeholders.	The IRP contains some guidance on the reporting of lessons learned, including at least half of the following: • Reporting instructions for lessons learned to stakeholders as outlined by the roles and responsibilities during an incident • A defined breakdown of the information that should be reported to stakeholders • Contact information for all relevant stakeholders.	The IRP does not contain guidance on the reporting of lessons learned. *AND/OR* The guidance provided does not provide sufficient detail to be considered 'partially implemented.'
Does the IRP include guidance on calculating and reporting a Mean-Time-To-Recover (MTTR)? ***(Medium)***	The IRP contains guidance on calculating and reporting a MTTR.	The IRP contains guidance on reporting a MTTR.	The IRP does not contain guidance on calculating or reporting an MTTR.

Questions

The Department has a dedicated team to work with the owners and operators of Systems of National Significance to ensure the Enhanced Cyber Security Obligations are well understood and appropriately applied, and that entities are meeting their obligations under the SOCI Act.

For further information please contact us at : **sons@homeaffairs.gov.au**



Australian Government

Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE