Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Enhanced Cyber Security Obligations – Vulnerability Assessments

Part 2C Division 4 *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 Vulnerability Assessment 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 Vulnerability Assessment 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 (the 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 a Vulnerability Assessment?

A vulnerability assessment is a process to identify and analyse weaknesses or gaps in a network or system that may expose critical infrastructure assets to a cyber security incident. Vulnerability assessments can take many forms, for example, a document-based review of a system's design, a hands-on assessment, or automated scanning with software tools.

Vulnerability assessments are integral to the security of a SoNS. They can help entities identify where further resources and capabilities are required to improve their preparedness for, and resilience to, cyber incidents. For example, a vulnerability assessment may inform recommendations on how to improve the responsible entity's incident response plan and future cyber security exercises.

They can also assist Government to understand whether cyber security advice or assistance can be provided to strengthen the security of SoNS, and identify patterns of weakness across sectors and assets which could be exploited by malicious actors.

All critical infrastructure entities, particularly those responsible for SoNS, should be conducting regular scans and testing for vulnerabilities on their systems and mitigating identified risks, in addition to regularly reviewing and actioning the Australian Signals Directorate's (ASD) alerts and advisories.

What is the Vulnerability Assessment obligation under the SOCI Act?

The Secretary of the Department of Home Affairs (or a delegate) may, by written notice, require a responsible entity to undertake a vulnerability assessment that relates to one or more of their SoNS within a certain timeframe.

Before applying the Vulnerability Assessment obligation, the Secretary must consult the responsible entity and consider the cost, reasonableness and proportionality of applying the obligation, as well as any other matters the Secretary considers relevant.

If the obligation is applied, the notice will specify whether the vulnerability assessment should be in relation to all types of cyber security incidents or one or more specified types of cyber security incidents (subsections 30CU(1) and 30CU(2) respectively). A vulnerability assessment undertaken as part of subsections 30CU(1) or 30CU(2) seeks to find gaps or weaknesses in the system, even if no exploitation of the vulnerability has been attempted. The notice will also specify the timeframe in which the vulnerability assessment must be undertaken.

Section 12M of the Act defines a *'cyber security incident'* as one or more acts, events or circumstances involving any of the following:

- unauthorised access to computer data or a computer program;
- unauthorised modification of computer data or a computer program;
- unauthorised impairment of electronic communication to or from a computer;
- unauthorised impairment of the availability, reliability, security or operation of a computer; or computer data; or a computer program.

After completion of the vulnerability assessment, the entity must provide a copy of the vulnerability assessment report to the Secretary within 30 days (or longer if specified in the written notice).

In practice, a notice in relation to all types of cyber security incidents (subsection 30CU(1)) would likely involve a broad spectrum assessment. In contrast, a notice in relation to one or more specified cyber security incidents (subsection 30CU(2)) would likely be used for a targeted assessment relating to specific information or intelligence.

Vulnerability assessment report

A report must be provided to the Secretary after the completion of a vulnerability assessment.

Entities should provide their vulnerability assessment report and any supporting documents via the Department's **secure upload portal**.

The purpose of the report is to provide an evaluation of the potential weaknesses or gaps in assets that are of highest criticality to Australia's national interests. Vulnerability assessment reports will also provide Government broader visibility of vulnerabilities and risks across industry to cyber threats.

The vulnerability assessment report must be a written document that assesses the vulnerability of the system to the type or types of cyber security incidents listed in the notice. The Department has not prescribed a specific template or any other requirements relating to the vulnerability assessment report. However, to assist in completing this report we recommend including the following:

- a high-level summary of the vulnerability to the types of cyber security incidents which were tested for, the parts of the network assessed, any vulnerabilities discovered, the criticality of any vulnerabilities discovered, and a traffic-light assessment of the difficulty/cost of mitigating the vulnerability;
- testing methodologies and a detailed explanation of the results of the vulnerability assessment; and
- recommendations and remedial actions that have or will be implemented to address any vulnerabilities discovered.

See pages **12 - 20** for further guidance on what may be included in a vulnerability assessment report.

Designated officers

The Vulnerability Assessment ECSO also enables the Secretary to request that a vulnerability assessment be undertaken by a designated officer. This could occur if the Secretary has reasonable grounds to believe that the responsible entity is incapable of complying with the vulnerability assessment notice or has not complied with a previous vulnerability assessment notice. Incapable of complying may mean an entity does not have the technical ability, resources or expertise to undertake the vulnerability assessment.

Designated officers are employees of the Department of Home Affairs or staff members of the ASD appointed by the Secretary to be a designated officer under the SOCI Act.

Under section 30CW of the Act, an entity may be required to engage with designated officers in relation to a vulnerability assessment in the following ways:

- provide designated officers access to the premises for the purpose of undertaking the vulnerability assessment;
- provide designated officers with access to computers for the purposes of undertaking the vulnerability assessment;
- provide the designated officer with reasonable assistance and facilities that are reasonably necessary to allow the designated officer to undertake the vulnerability assessment.

If a designated officer undertakes a vulnerability assessment, they will also be required to complete the associated vulnerability assessment report. Responsible entities will be given an opportunity to contribute to and review the vulnerability assessment report undertaken by the designated officer.

Entities must be consulted prior to a designated officer being appointed.

The Department's approach

The initial approach to the Vulnerability Assessment obligation

The Department's initial approach to the Vulnerability Assessment ECSO is focused on responding to the most critical threats and risks to SoNS. This will include potential or known vulnerabilities in information and operational technology systems that if exploited could have serious consequences to the availability, integrity and reliability of the SoNS or the confidentiality of its information.

To achieve this, the Department may apply this obligation in response to intelligence, such as an ASD critical alert or information from other partners in relation to a known or suspected threat, vulnerability or incident that represents a significant risk to Australia's critical infrastructure.

The obligation will be applied under subsection 30CU(1) of the Act, requiring an entity to undertake a broad-based vulnerability assessment in relation to all types of cyber security incidents, or subsection 30CU(2) requiring a more targeted assessment in relation to a specified type (or types) of cyber security incidents.

When applying the Vulnerability Assessment ECSO, the Department will:

- apply the obligation on rare and exceptional occasions, where the exploitation of a known or potential vulnerability could lead to a serious cyber security incident and there is information to suggest Australia's critical infrastructure could be targeted and/or significantly impacted;
- undertake consultation with responsible entities and relevant Commonwealth regulators, noting that the consultation period may be short and/or verbal and may include briefings from security agencies;
- where possible, include supporting information at the OFFICIAL or OFFICIAL: SENSITIVE levels to support the entity's understanding of a known or potential vulnerability;
- not prescribe, but may recommend, the type of vulnerability assessment or the manner in which it must be undertaken;
- not prescribe, but may recommend, remedial or mitigation measures; and
- not prescribe a specific template for the vulnerability assessment report.

There are currently no requirements specified in SOCI rules regarding the type or manner in which a vulnerability assessment must be undertaken. As the purpose of this obligation is to assist entities to identify any gaps or weaknesses in their systems that may lead to the SoNS being subject to a cyber security incident, the Department will provide as much information as possible to support the entity's understanding of the known or potential vulnerabilities.

While entities will be able to determine the type and format of vulnerability assessment they undertake, entities should ensure it is reasonable based on the circumstances and information provided.

Depending on the circumstances, the obligation could be applied in relation to an individual SoNS, all SoNS within a particular sector or asset class, or to all SoNS. For example, the obligation may be applied in relation to SoNS within the energy sector only, if there is a particular vulnerability identified in a software program that is widely used by the energy sector to support their operational technology systems. A previous example that may have met the threshold (as described above in

this section) to apply the Vulnerability Assessment obligation includes the Log4j vulnerability due to its broad reach and high rate of exploitation at the time[1].

The Department acknowledges that many SoNS entities embed a program of regular vulnerability management and scanning of their critical systems. The Department will not seek to apply this obligation where it is not required. During the consultation period, responsible entities will be able to provide evidence that they have already undertaken a vulnerability assessment that would meet the Vulnerability Assessment ECSO should it be applied, or that the vulnerability does not apply to their SoNS assets (for example, if an organisation does not use particular software that is subject to the vulnerability). Entities will also be consulted on the proposed timeframes in which the vulnerability assessment should be undertaken and will have an opportunity to provide feedback on the practicality and feasibility of such timeframes.

Future application of the Vulnerability Assessment obligation

In the future, the Vulnerability Assessment ECSO could be applied in a manner that requires responsible entities to conduct routine and regular vulnerability assessments over a specified period of time.

Rules could also prescribe a specific type or form of vulnerability assessment that must be undertaken, or the format or content of the vulnerability assessment report.

Consultation must occur prior to the obligation being applied in this manner.

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 and mitigating cyber security incidents that could have a relevant impact on their systems.

The CISC's 2024-25 Compliance Regulatory Posture relating to the Enhanced Cyber Security Obligations will continue to focus on partnering with the entities responsible for SoNS. For more information see **SOCI Compliance Regulatory Posture 2024** and **our regulatory principles and approach (cisc.gov.au)**

[1] For further information on the Log4J vulnerability see: 2021-007: Log4j vulnerability – advice and mitigations | Cyber.gov.au and CSRB Report on Log4j - Public Report - CISA

Applying the obligation

What to expect: a step-by-step guide

1 Consultation

Responsible entities will receive notification from the Department advising that the Secretary (or a delegate) is considering applying the Vulnerability Assessment obligation.

Consultation may be verbal, short and will be determined based on the urgency and criticality of the potential vulnerability.

The Secretary must consider the costs, reasonableness and proportionality of applying the obligation.

The Secretary will also consider the size and complexity of the organisation and assessment required and any resourcing constraints relating to third party providers.

Entities and relevant Commonwealth regulators will be invited to provide feedback to the Department as part of the consultation process.

Consultation timeframe – the SOCI Act does not specify a minimum timeframe for consultation under this provision. The Department will clearly specify the timeframe in the notification.

Consultation form – given the time critical nature of some cyber threats and risks, the consultation process for the Vulnerability Assessment ECSO is likely to be different to that for the other ECSOs. For time critical cyber threats, the consultation period may be short and may include briefings from security agencies at short notice. The Department will seek to provide as much information as possible at the OFFICIAL or OFFICIAL: SENSITIVE levels to support the entity's understanding of any identified issues. This may include ASD alerts or advisories.

What type of information should entities provide during the consultation period – entities should consider the cost and practicalities of undertaking the vulnerability assessment and providing a vulnerability assessment report. Entities may wish to provide evidence that they have already undertaken a vulnerability assessment and, where necessary, taken remedial action. Entities may also wish to demonstrate that the cyber security incident referenced within the proposed notice would not impact their SoNS assets as they do not use, for example, the particular software named in the notice.

2 The obligation is applied

Following the consultation process, the responsible entity will receive a written notice from the Secretary advising whether or not the obligation has been applied. If it has been applied, the responsible entity will be required to undertake a vulnerability assessment within the timeframe specified in the written notice.

Timeframe – the timeframe specified in the notice to undertake the assessment will be based on the particular threat, as well as any feedback provided during the consultation period.

Requirements – there are no requirements currently specified in the rules regarding the type of vulnerability assessment that must be undertaken (eg: host assessment or network assessment) or the manner in which the vulnerability assessment must be undertaken (eg: automated scanning or penetration testing). Noting the purpose of this obligation is to assist entities to identify any gaps or weaknesses in their systems that may lead to the SoNS being subject to a cyber security incident, the Department will provide as much information as possible to support the entity's understanding of the known or potential vulnerability. Entities should ensure the vulnerability assessment undertaken is reasonable based on the circumstances and information provided.

What if an entity undertakes the vulnerability assessment prior to a notice being given – it is not the Department's intent to require an entity to re-do a vulnerability assessment. In these circumstances the Department will work with the entity to ensure the purpose of the ECSO is achieved. This may include accepting a vulnerability assessment that occurred prior to a notice being given as compliant with the obligation, or seeking voluntary agreement that the entity will provide a vulnerability assessment report to the Department within a specified timeframe. This will be determined on a case-by-case basis.

3 Undertake VA assessment and prepare VA report

The responsible entity will be required to undertake the vulnerability assessment and prepare a vulnerability assessment report. The report must be provided to the Secretary within the time specified in the notice.

Timeframe – the SOCI Act requires that the entity prepare and give a copy of the vulnerability assessment report to the Secretary within 30 days after the vulnerability assessment was conducted (or longer if the Secretary allows). The timeframe to provide the report will be specified in the notice. The timeframe will be determined by the particular threat and vulnerability being considered, as well as any information from the entity regarding the reasonableness, practicality and feasibility of meeting the timeframe.

Report requirements: there is no mandated template for this report, nor are there any requirements specified in the rules of what should be in the report. The purpose of the report is to assess the vulnerability of the SoNS to cyber security incidents. The Department has provided recommendations to assist entities complete the report – see pages **12 – 20.**

Alignment with Directions under the Protective Security Policy Framework

The Department of Home Affairs is responsible for administering the Protective Security Policy Framework (PSPF).

To support the uplift of cyber security across the Commonwealth Government – a key initiative in the ***2023-2030 Australian Cyber Security Strategy*** – the Secretary of the Department of Home Affairs may issue Directions to Australian Government entities under the PSPF, requiring them to manage protective security risks to either their systems, information or assets.

There are two types of PSPF Directions:

- Administrative Directions – issued to mitigate general security threats that present a significant risk to the Australian Government that require urgent action.

- Emergency Directions – issued to mitigate a known or reasonably suspected security threat, vulnerability or incident that represents a significant risk to the Australian Government and/or to require information to inform a whole of government response such as confirming a patch has been updated.

While the PSPF Directions are not part of the SOCI Act or the ECSO framework, the advice contained in these Directions are in many instances relevant to critical infrastructure entities. PSPF Directions are published on the Department of Home Affairs **website**.

The Department may amplify a PSPF Direction with the SoNS cohort and encourage entities to follow a similar course of action, should they determine their systems may also be impacted.

By sharing these Directions, we will complement the existing information sharing measures established via the SoNS framework and SoNS Trusted Information Sharing Network (TISN).

Protecting sensitive information

What documentation do responsible entities need to provide?

The responsible entity is required to provide a copy of their vulnerability assessment report to the Secretary. The responsible entity may also choose to provide additional documents related to their vulnerability assessment, including asset inventories, automated tool outputs, penetration testing findings, and any mitigation or upgrade implementation plans.

This can be done securely via the Department's **secure upload portal.** The development and submission of the vulnerability assessment report is a once off requirement, entities are not required to provide continuous or updated reports to the Secretary.

What will the Department do with an entity's vulnerability assessment report?

The Department will review the vulnerability assessment report to:

- determine whether it meets the requirements of the Vulnerability Assessment obligation as applied in relation to the SoNS and as set out in the written notice;
- understand the vulnerability assessment maturity of SoNS responsible entities within certain sectors and across the SoNS cohort as a whole;
- identify opportunities to support cyber security uplift of an entity, a sector or all SoNS;
- determine if any rules are required to uplift the vulnerability assessment capabilities of an entity, a sector or all SoNS;
- inform considerations on the need for the vulnerability assessment to be managed by a designated officer.

Additionally, the Department may share vulnerability assessment reports with the ASD which would assist the Government to build a collective picture of the nature of threats against specific sectors or particular SoNS assets.

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

Entities should provide their vulnerability assessment report and any supporting documents via the Department's **secure upload portal.**

The portal has been developed to ensure that sensitive information provided for the purpose of meeting the ECSO requirements are immediately safe dropped to a secure location on the Australian Government's SECRET Network. The information will **not** be removed from the SECRET network.

For more information regarding the safety of ECSO information provided to the Department, please contact **sons@homeaffairs.gov.au**.

Vulnerability Assessments – What Good Looks Like

Overview

- The below framework provides guidance to entities when planning, undertaking and evaluating a vulnerability assessment. It is **not** mandatory and should be used as guidance only.
- Vulnerability assessments can take many forms, for example, a document-based review of a system's design, a hands-on assessment, or automated scanning with software tools. The criterion or considerations outlined in the guidance may not be relevant in every scenario.
- A SoNS responsible entity that is subject to the Vulnerability Assessment ECSO should carefully consider the information in the written notice when undertaking the assessment and developing the report.
- Organisations not subject to the Vulnerability Assessment ECSO may also find this guidance useful to support best practice when planning, undertaking and evaluating vulnerability assessments.

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 conducting vulnerability assessments.

The Criteria

Criterion code	Criterion name
VA.1	Alignment to responsible entity's cyber security strategy and/or risk management framework
VA.2	Scope of the vulnerability assessment
VA.3	Alignment between methodology and the environment/vulnerability being tested
VA.4	High-level findings
VA.5	Analysis of the results of the vulnerability assessment
VA.6	Raw data output from the vulnerability assessment
VA.7	Remediation actions/recommendations
VA.8	Impact on responsible entity's cyber roadmap/uplift program
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 when planning, undertaking and evaluating a vulnerability assessment.

Criterion VA.1: Alignment to responsible entity's cyber security strategy and/or risk management framework

Outcome

For SoNS responsible entities' subject to a vulnerability assessment notice, the assessment must align to the information in that notice.

More generally, vulnerability assessments should be informed by the organisation's wider cyber security strategy and/or risk management program to ensure that they are producing the most efficient cyber security outcomes. For example, responsible entities should prioritise assessing the most business-critical systems identified during the development of their cyber security strategy and/or risk management program. Similarly, the outcomes of the vulnerability assessment should inform future development of the cyber security strategy and/or risk management program.

An effective cyber security strategy will identify the threat vectors, threat actors and risk environment factors that are most likely to cause a serious cyber security incident on a particular SoNS. Identifying the most likely tactics, techniques and procedures that will be used against a SoNS will allow defenders to undertake a vulnerability assessment that is targeted towards the vulnerabilities and exploits utilised by relevant threat actors and allow entities to more accurately assess system vulnerabilities to cyber security incidents.

Cyber security exercises may also inform the vulnerabilities and assets that should be prioritised for assessment. Recent exercises may have identified potential vulnerabilities or weaknesses in the SoNS' network. Conversely, vulnerability assessment outcomes may inspire cyber security exercises, or changes to incident response plans.

Finally, the vulnerability assessments should be aligned to the testing and assurance program used by the responsible entity under any relevant regulatory or security framework requirements. For example, the Essential Eight has a requirement for regular vulnerability scans.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the assessment align to the wider cyber security strategy? ***(High)***	The vulnerability assessment is informed by the cyber security strategy and the outcomes of the assessment are integrated into the cyber security strategy. The assessment report describes this alignment.	The vulnerability assessment is partially informed by the cyber security strategy *AND* The outcomes of the assessment are integrated into the cyber security strategy. The assessment report describes this partial alignment.	The vulnerability assessment is not informed by the cyber security strategy and the outcomes of the assessment are not integrated into the cyber security strategy. *AND/OR* The assessment report does not describe any alignment.
Does the assessment align to a security testing and assurance program? ***(Medium)***	The vulnerability assessment outcomes align to the overall security testing and assurance program. The assessment report describes this alignment.	The vulnerability assessment outcomes partially align to the overall security testing and assurance program. The assessment report describes this partial alignment.	There is no explicit alignment between the vulnerability assessment outcomes and the overall security testing and assurance program. *OR* The assessment report does not describe the alignment between the vulnerability assessment outcomes and the overall security testing and assurance program.

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the assessment align to recent or planned threat assessment outcomes? ***(Medium)***	The assessment report explains how the vulnerability assessment was informed by a recent threat assessment and the results of the vulnerability assessment have been integrated into the SoNS' threat profile. *AND* An established Vulnerability Register or Record has been maintained.	The report explains how the vulnerability assessment was informed by a recent threat assessment. *AND* An established Vulnerability Register or Record has been maintained, but with some actions missing.	The report does not include any details about the alignment between the vulnerability assessment and the SoNS' threat profile. *AND* An established Vulnerability Register or Record has not been implemented.

Criterion VA.2: Scope of the vulnerability assessment

Outcome

Vulnerability assessments should focus on network areas that are most business-critical and could result in the occurrence of a cyber security incident if exploited by a malicious actor. It would not be useful for a responsible entity to undertake a vulnerability assessment of parts of the network that cannot be affected by a particular vulnerability, for example, looking for a Linux vulnerability on a Windows machine.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Are all parts of the network that were assessed or not assessed described in the vulnerability assessment report? ***(Critical)***	The report identifies, listed by hostname with an accompanying description, all the parts of the network that were included in the assessment and an accompanying justification of any parts of the network that were/were not assessed.	The report identifies, in any format, the parts of the network that were included or not included in the assessment.	The report does not identify the parts of the network that were or were not assessed.
Were all parts of the network present in the tool output included in the report? (if applicable) ***(High)***	All devices related to SoNS assets that appear in the tool output are present in the report, either as part of the assessment or with justification for why they were not included. If parts of the network are unable to have an active vulnerability scan, the report includes what sections are excluded or have had manual vulnerability assessment conducted.	Tool output is not provided for all tools used in the assessment, or is otherwise incomplete.	Some devices related to SoNS assets that appear in the tool output are not present in the report. *OR* No tool output is provided.

Criterion VA.3: Alignment between methodology and the environment/vulnerability being tested

Outcome

Vulnerability assessments should use an appropriate assessment methodology. Specific methodology and/or software tools may be needed for different environment types or to assess for certain vulnerabilities in relation to specific types of cyber security incidents.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Was the appropriate methodology used for this vulnerability assessment? ***(Critical)***	The vulnerability assessment report details the methodology that was used in the assessment and why that methodology was the most appropriate. It also details regulatory/compliance requirements.	The vulnerability assessment report details the methodology that was used in the assessment. Regulatory/ compliance requirements are either partially or not mapped.	The vulnerability assessment report does not provide details on the methodology that was used in the assessment and regulatory/compliance requirements are not mapped.
Is there evidence that the methodology or tool being used can accurately identify the vulnerability and environment being assessed? ***(Medium)***	The report uses previous examples to describe how this methodology is appropriate for the vulnerability and environment being assessed. If no specific vulnerabilities were being assessed, the report briefly outlines what kinds of vulnerabilities the assessment methodology was likely to uncover.	The report gives a hypothetical explanation as to why this methodology is appropriate for the vulnerability and environment being assessed.	The report does not explain the appropriateness of the methodology for the vulnerability and environment being assessed.
Does the responsible entity undertaking the vulnerability assessment state their confidence that if the vulnerability were present on the system being assessed, it would have been found? ***(Medium)***	The report provides a confidence assessment, presented in a percentage format, that if the vulnerability were present on the system being assessed, it would have been found.	N/A.	The report does not provide a confidence assessment, presented in a percentage format, that if the vulnerability were present on the system being assessed, it would have been found.

Criterion VA.4: High-level findings

Outcome

The vulnerability assessment report should contain high-level findings that would be appropriate for non-technical stakeholders to understand. These findings should outline the vulnerability of the system to the types of cyber security incidents which were tested for, the parts of the network assessed, any vulnerabilities discovered, the criticality of any vulnerabilities discovered, and a traffic-light assessment of the difficulty/cost of mitigating the vulnerability.

The high-level findings will repeat information included in other sections of the report. The high-level findings are intended to be read as a summary for executive stakeholders.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the report list the specific vulnerability or vulnerabilities that are being assessed? ***(Critical)***	The vulnerability report contains a summary list of vulnerabilities which informed the planning of the assessment. Vulnerabilities in	The vulnerability reports contain a high-level overview of vulnerabilities which informed the planning of the assessment but not all risk	The vulnerability assessment report does not contain a summary list of vulnerabilities which informed the planning of the assessment.

Consideration	Well Implemented	Partially Implemented	Not Apparent
	the list are labelled with a criticality rating, impact, and details of previous mitigations. If no specific vulnerabilities were being assessed, the report briefly outlines what kinds of vulnerabilities the assessment methodology was likely to uncover.	ratings, impacts, or details of previous mitigations are provided.	
Does the report consider the consequences/impact of any detected vulnerabilities against the cyber security incident type or types contained within the ECSO notice? ***(Critical)***	The report explicitly considers all possible consequences of any detected vulnerabilities against the cyber security incident type or types contained in the ECSO notice.	The report considers some possible consequences of any detected vulnerabilities against the cyber security incident type or types contained in the ECSO notice.	The report does not consider the possible consequences of any detected vulnerabilities against the cyber security incident type or types contained in the ECSO notice.
Does the report list high-level sections of the network being targeted by the vulnerability assessment and detail any sections that have been excluded? ***(Critical)***	The report lists the sections of the network that were assessed. The report lists these in a manner that is accessible and meaningful to non-technical stakeholders, such as business unit names or OT systems that were assessed. The report also lists any sections that have been excluded and notes why these sections have been excluded. *Note:* Although this information is requested in a hostname format in criterion VA.2, this information should also be included in a separate section for a non-technical audience.	The report lists the sections of the network that were assessed. It does not list the sections that were excluded.	The report does not list the sections of the network that were assessed.
Does the report summarise the vulnerabilities that were discovered during the assessment? ***(Critical)***	The report includes a section outlining any vulnerabilities discovered, including, for example: • Common Vulnerabilities and Exposures (CVE) references • Common Vulnerability Scoring System (CVSS) severity score • Common Weakness Enumeration (CWE). If no vulnerabilities were detected, the consideration is marked as well implemented.	The report includes a section outlining the vulnerabilities discovered, but does not include, for example: • Common Vulnerabilities and Exposures (CVE) references • Common Vulnerability Scoring System (CVSS) severity score • Common Weakness Enumeration (CWE).	If vulnerabilities were discovered, the report does not include a section outlining any vulnerabilities discovered.

Criterion VA.5: Analysis of the results of the vulnerability assessment

Outcome

The vulnerability assessment report should include a detailed explanation of the results of the vulnerability assessment. This explanation should be directed at a technical audience. This section should contain more technical detail and cover more areas than the high-level findings. Information contained in the high-level findings should be duplicated in this section so that readers do not need to read both sections to have all relevant information.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the report contain a detailed description of vulnerabilities discovered? ***(Critical)***	This section includes a detailed description of vulnerabilities discovered, including all of the following: • Consequences of the vulnerabilities • Likelihood of the vulnerabilities being exploited (including whether a known exploit exists) • Methods to exploit the vulnerabilities • Mitigation/remediation strategies Where applicable, the vulnerabilities' Common Vulnerabilities and Exposures (CVE) ID number.	This section includes a description of vulnerabilities discovered, including some of the following: • Consequences of the vulnerabilities • Likelihood of the vulnerabilities being exploited • Methods to exploit the vulnerabilities • Mitigation/remediation strategies Where applicable, the vulnerabilities' Common Vulnerabilities and Exposures (CVE) ID number.	This section does not include a description of vulnerabilities discovered. It does not include any of the following: • Consequences of the vulnerabilities • Likelihood of the vulnerabilities being exploited • Methods to exploit the vulnerabilities • Mitigation/remediation strategies Where applicable, the vulnerabilities' Common Vulnerabilities and Exposures (CVE) ID number.
Does the report contain an assessment about the likelihood of vulnerabilities being exploited? ***(Critical)***	This section includes a detailed assessment of the likelihood of vulnerabilities being exploited, ensuring the following factors are considered: • Existing cyber security infrastructure • Ubiquity or rarity of underlying technology • Availability of existing POC exploit code • Ease of access • Ease of exploitation. *Note:* It is recommended that the NIST SP 800-30 likelihood assessment scale be used. Where the responsible entity is using a different set of likelihood definitions, this should be made clear.	This section includes an assessment of the likelihood of vulnerabilities being exploited, with some of the following factors considered: • Existing cyber security infrastructure • Ubiquity or rarity of underlying technology • Availability of existing POC exploit code • Ease of access • Ease of exploitation.	This section does not include an assessment of the likelihood of vulnerabilities being exploited, with none of the following factors considered: • Existing cyber security infrastructure • Ubiquity or rarity of underlying technology • Availability of existing POC exploit code • Ease of access • Ease of exploitation.
Does the report contain the information about the systems affected by the vulnerabilities? ***(Critical)***	The section includes all vulnerabilities discovered and the corresponding systems that are affected.	The section includes some vulnerabilities and the corresponding systems that are affected.	The section does not mention vulnerabilities and the corresponding systems that are affected.
Does the report detail the exploitation impact on the operation of the SoNS? ***(Critical)***	This section details the exploitation impact on the operation of the SoNS, for example: • How exploitation of systems affected by vulnerabilities would impact the operation of the SoNS • How vulnerabilities directly impact the SoNS and its services • The criticality of the impact on the SoNS.	This section addresses some of the exploitation impacts on the operation of the SoNS, for example: • How systems affected by vulnerabilities impact the SoNS • How vulnerabilities directly impact the SoNS and its services • The criticality of the impact on the SoNS.	This section addresses zero or one of the exploitation impacts on the operation of the SoNS, for example: • How systems affected by vulnerabilities impact the SoNS • How vulnerabilities directly impact the SoNS and its services • The criticality of the impact on the SoNS.
Does the vulnerability assessment report detail the effects each vulnerability has	The report includes the aspects of the CIA Triad (Confidentiality, Integrity, Availability) that are affected;	The report includes one of the aspects of the CIA Triad (Confidentiality, Integrity, Availability) that is affected;	The report includes none of the aspects of the CIA Triad (Confidentiality, Integrity, Availability) that are affected;

Consideration	Well Implemented	Partially Implemented	Not Apparent
to each of the sections of the CIA triad? ***(Medium)***	and the CVSS score (Common Vulnerability Scoring System) is applied to all of the assessed vulnerabilities.	and the CVSS score (Common Vulnerability Scoring System) is applied to the assessed vulnerabilities.	and the CVSS score (Common Vulnerability Scoring System) is not applied to the assessed vulnerabilities.

Criterion VA.6: Raw data output from the vulnerability assessment

Outcome

The vulnerability assessment report may include the raw output of the vulnerability scan/assessment tool as an appendix or a separate supporting file.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the vulnerability assessment report include the vulnerability scan/assessment tool raw data output? ***(High)***	The report includes (either in the appendix or an attached file) the raw data output from every scanning tool used in the vulnerability assessment. If no tool was used that produces a data output, the consideration is marked as well implemented.	Some tool output is provided, but some tools which are listed in the report do not have output provided. Raw tool output does contain some but not all the categories described in the instructions.	The report does not include the raw data output from a scanning tool that was used in the vulnerability assessment.
Do the contents of the raw tool output files validate the contents of the vulnerability report? ***(High)***	Sufficient evidence in the raw tool output is given to validate the contents of the vulnerability report, containing all the following categories: • What times the tools were run • Information to replicate the assessment • Whether the scans were authenticated (show the percentage value).	Some sufficient evidence in the raw tool output is given to validate the contents of the vulnerability report, containing some of the following categories: • What times the tools were run • Information to replicate the assessment • Whether the scans were authenticated (show the percentage value).	There is no evidence in the raw tool output to validate the contents of the vulnerability report, as it contains none of the following categories: • What times the tools were run • Information to replicate the assessment • Whether the scans were authenticated (show the percentage value).
Has there been any changes to the data? ***(High)***	There have been no changes to the raw data output and logs provide evidence to support this.	There is insufficient evidence in the logs to determine whether changes have been made to the raw data.	There is evidence of changes to the raw data output.
Could there have been any changes made to the data? ***(Medium)***	The report details prevention methods in place, how the integrity of the data was maintained from end-to-end, and provides logs for all tools.	The report details some prevention methods in place, mentions integrity is maintained but not how, and is missing logs for some tools.	The report does not state prevention methods in place, how integrity is maintained, and is missing all logs.

Criterion VA.7: Remediation actions/recommendations

Outcome

A key outcome of the vulnerability assessment report is to plan and document remediation activities. The actions taken to remediate vulnerabilities identified in the assessment should outline estimated timelines, costs, and any potential impact on the availability of the asset or assets.

The vulnerability assessment should inform recommendations on how to improve the responsible entity's incident response plan and future cyber security exercises. The assessment may provide information on new vulnerabilities and potential weaknesses in systems that should be considered in an incident response plan. Although vulnerability assessments can identify the existence of an

exploitable vulnerability within a system, a cyber security exercise may be necessary to accurately identify a responsible entity's ability to respond to the exploitation of a vulnerability.

Considerations

Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the vulnerability assessment report contain what actions were taken or are planned to be taken to remediate any vulnerabilities identified? ***(Critical)***	The vulnerability report includes supporting instructions for how mitigation activities should be achieved for all of the identified vulnerabilities and a documented plan of action to address vulnerabilities.	The vulnerability report includes supporting instructions for how mitigation activities should be achieved for some of the identified vulnerabilities. There are some key factors missing from the documentation outlining the plan for addressing vulnerabilities.	The vulnerability report does not include supporting instructions for how mitigation activities should be achieved for any of the identified vulnerabilities, and there is no documented plan of action to address vulnerabilities.
Does the report contain any recommendations to update the incident response plan? ***(Medium)***	If a vulnerability was detected, the report outlines any planned updates to the incident response plan. If no updates to the IRP are required, the report explains why. If no vulnerability was detected, the consideration is marked as well implemented.	N/A.	If a vulnerability was detected, the report does not outline any planned updates to the incident response plan and does not explain why no updates were required.
Does the report contain any recommendations to undertake or improve cyber security exercises? ***(Medium)***	If a vulnerability was detected, the report outlines any planned or modified cyber security exercises. If no exercises are required, the report explains why. If no vulnerability was detected, the consideration is marked as well implemented.	N/A.	If a vulnerability was detected, the report does not outline any planned or modified cyber security exercises and does not explain why no updates were required.

Criterion VA.8: Impact on responsible entity's cyber roadmap/uplift program

Outcome

Cyber security for SoNS should be guided by cyber security roadmaps or uplift programs. The results of a vulnerability assessment may require the reallocation of resources that could impact on other cyber security projects.

The vulnerability assessment report should, to the best of the responsible entity's ability, outline how the vulnerability assessment results will likely impact on the responsible entity's cyber security roadmap or uplift program.

Considerations

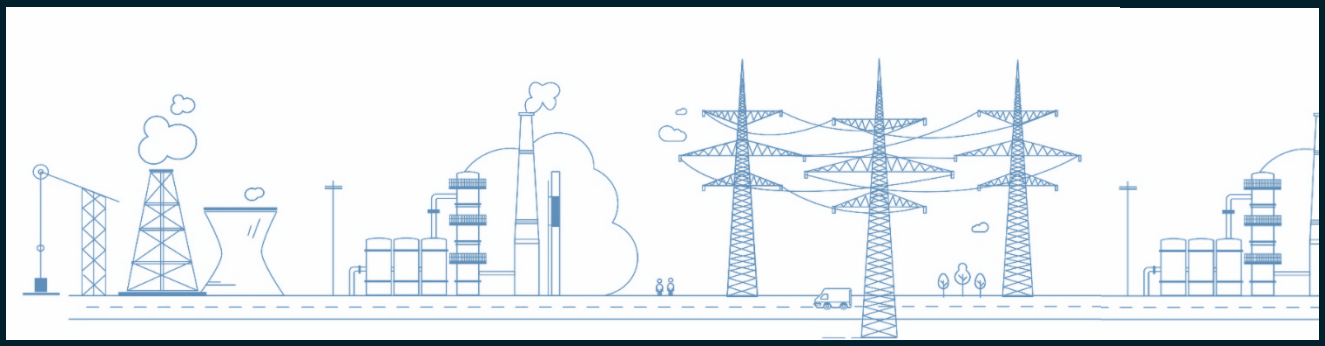
Consideration	Well Implemented	Partially Implemented	Not Apparent
Does the report describe an integration of recommendations into an existing cyber security roadmap? ***(Medium)***	The report includes a section that describes how any findings from the vulnerability assessment affect and/or will be integrated into, an existing cyber security roadmap/strategy, including remediation activities. If no change is required, the report explains why.	The responsible entity supplied an uplift program with roadmap containing a few goals. The vulnerability report mentions that remediation activities should or will be integrated into the existing cyber security uplift program but does not describe steps or a plan to complete this.	The report does not outline how any findings from the vulnerability assessment affect or will be integrated into an existing cyber security roadmap.

Consideration	Well Implemented	Partially Implemented	Not Apparent
	If the responsible entity does not have a cyber security strategy or roadmap, there should be a recommendation to establish one.		
When justifying the new recommendations, does the report include consideration to the recommended changes' effect upon other existing or planned cyber security efforts? ***(Medium)***	The report includes a section that details how the integration of any results from the assessment would impact on existing planned cyber security efforts, including all of the following: • Criticality of the recommendation • Resource requirements • Financial cost of remediation. If the responsible entity does not have a cyber security strategy or roadmap, there should be a recommendation to establish one.	The report includes a section that describes remediation activities, but little to no detail on how to do this.	The vulnerability report does not detail how a discovered vulnerabilities' remediation activities should be completed.

Questions

The Department of Home Affairs 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