

Administration of Critical Infrastructure Protection Policy

Department of Home Affairs

© Commonwealth of Australia 2022

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-741-4(Print)

ISBN 978-1-76033-742-1 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Senior Executive Director
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:

communication@anao.gov.au.



Canberra ACT
21 June 2022

Dear Mr President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Department of Home Affairs. The report is titled *Administration of Critical Infrastructure Protection Policy*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — <http://www.anao.gov.au>.

Yours sincerely



Grant Hehir
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
<http://www.anao.gov.au>

Audit team

Glen Ewers
Rebecca Helgeby
Jessica Kanikula
Edwin Apoderado
Ji Young Kim
Alex Wilkinson

Contents

Summary and recommendations.....	7
Background	7
Conclusion	8
Supporting findings	8
Recommendations	9
Summary of entity response	11
Key messages from this audit for all Australian Government entities	11
Audit findings.....	13
1. Background	14
Introduction	14
Critical infrastructure policy and regulation	14
Rationale for undertaking the audit	21
Audit approach	21
2. Governance arrangements	23
Are risks to critical infrastructure assets identified and managed effectively?	23
Have effective coordination arrangements with key stakeholders been established?	29
Has an effective performance framework been established?	33
3. Compliance activities	39
Has an effective framework been established to manage compliance with critical infrastructure requirements?	39
Are effective procedures and systems in place to support the use of regulatory tools?	42
Is the use of regulatory tools consistent with legislative and procedural requirements?	44
Is there an effective process to identify non-compliance?	49
Has the use of regulatory tools been effectively reviewed?	53
Appendices	55
Appendix 1 Entity response	56
Appendix 2 Improvements observed by the ANAO	58
Appendix 3 Timeline of critical infrastructure reform events and implications	59
Appendix 4 Other jurisdiction critical infrastructure arrangements	62



Audit snapshot

Auditor-General Report No.38 2021–22

Administration of Critical Infrastructure Protection Policy



Why did we do this audit?

- ▶ This audit provides assurance to the Parliament on whether the Department of Home Affairs (the department), as policy and regulatory lead for critical infrastructure protection coordination, has an effective approach to protecting Australia's assets of national significance and supporting asset owners and operators to improve their resilience to attacks.
- ▶ The potential for an attack that degrades or disables a critical infrastructure asset has been identified by industry and governments in Australia and abroad.



Key facts

- ▶ Overseas terrorist attacks in 2001 and 2002 prompted formal government and industry engagement on critical infrastructure asset threat preparedness and response in Australia.
- ▶ The department estimates that the 168 assets registered as being critical infrastructure will increase ten-fold as a result of legislative changes in 2021.



What did we find?

- ▶ The department's administration and regulation of critical infrastructure protection policy was partly effective.
- ▶ The department had partly effective governance arrangements to administer critical infrastructure protection policy.
- ▶ Improvements are required on integrated risk management, development of stakeholder engagement strategy, and performance measurement.
- ▶ The department's administration of compliance activities consistent with critical infrastructure protection requirements is partly effective.



What did we recommend?

- ▶ The Auditor-General made seven recommendations to the department aimed at: the use of risk management to inform decision-making; establishing an engagement strategy; having appropriate performance measurement; improving the department's existing framework to manage compliance; and support and review the effective use of all available regulatory tools.
- ▶ The department agreed to all seven recommendations.

11

sectors covered by the *Security of Critical Infrastructure Act 2018*, expanded from four in 2021.

28 of 36

measures of control effectiveness indicators did not align with enterprise level critical infrastructure risk reporting.

15 of 22

policy and procedural documents to support critical infrastructure related compliance activities were not finalised and approved.

Summary and recommendations

Background

1. Ensuring the security and resilience of Australia's critical infrastructure is a responsibility shared by the Commonwealth, state and territory governments, infrastructure owners and operators.
2. The Department of Home Affairs (the department) is the lead Australian Government agency responsible for the administration of critical infrastructure policy and regulation. The Critical Infrastructure Centre was established in 2017 to coordinate the management of risks to Australia's critical infrastructure and deliver more coordinated national security assessments to inform foreign investment decisions in significant and complex cases.
3. In 2018, legislative coverage of critical infrastructure security was expanded from being considered primarily under the *Foreign Investment and Takeovers Act 1975*, to include regulation under:
 - the *Security of Critical Infrastructure Act 2018* (SoCI Act); and
 - amendments to Part 14 of the *Telecommunications Act 1997*, or Telecommunications Sector Security Reforms (TSSR).
4. On 2 December 2021, the SoCI Act was amended to increase its coverage from four to 22 asset classes, across 11 sectors. These amendments also introduced mandatory cyber incident reporting and a regime to respond to cyber incidents, the 'government assistance powers'. Additional amendments to the SoCI Act commenced on 2 April 2022 including:
 - a requirement for critical infrastructure assets to adopt and maintain a risk management program; and
 - providing the government with the power to declare certain critical infrastructure assets as Systems of National Significance to which Enhanced Cyber Security Obligations may apply.

Rationale for undertaking the audit

5. The potential for an attack that degrades or disables a critical infrastructure asset has been identified by industry and governments in Australia and abroad. This audit provides assurance to the Parliament on whether the department, as policy and regulatory lead for critical infrastructure protection coordination, has an effective approach to protecting Australia's assets of national significance, and supporting asset owners and operators to improve their resilience to attacks.

Audit objective and criteria

6. The audit objective was to assess the effectiveness of the department's administration and regulation of critical infrastructure protection policy. To form a conclusion against this objective, the following high-level criteria were applied.
 - Has the department established effective governance arrangements to administer critical infrastructure protection policy? (Chapter 2)

- Does the department effectively administer compliance activities consistent with critical infrastructure protection requirements? (Chapter 3)

Conclusion

7. The department's administration and regulation of critical infrastructure protection policy was partly effective.

8. The department has partly effective governance arrangements to administer critical infrastructure protection policy. Implementation of critical infrastructure related risk assessments and reporting was not captured in risk documentation. The effectiveness of the department's stakeholder coordination arrangements is reduced by not having an engagement strategy and providing limited support to other critical infrastructure regulators. The department's performance framework as it related to critical infrastructure was not adequate, with performance statements, regulatory performance assessment, and use of internal measures to inform policy and regulation requiring improvement.

9. The department's administration of compliance activities consistent with critical infrastructure protection requirements is partly effective. The department's compliance framework does not reflect existing responsibilities or compliance requirements. Compliance activities are not supported by approved procedures or systems controls. The department has not established a risk-based decision framework for achieving compliance outcomes or demonstrating its impact on asset security or resilience. The department does not have a process of effectively reviewing its use of regulation tools, impact on industry or to inform continuous improvement.

Supporting findings

Governance arrangements

10. The department identified key critical infrastructure risks and had appropriate governance arrangements to assess and assign responsibility for these risks. The department's critical infrastructure risk management does not represent an integrated approach to risk management between its enterprise and operational, legislative and policy functions. Implementation of critical infrastructure related risk assessments and reporting was not captured in risk documentation, which reduces its use to inform business planning, legislative reform, and policy decisions. (See paragraphs 2.3 to 2.23)

11. While the department undertakes coordination activities with key stakeholders, including through some long-established forums, it does not have a documented stakeholder engagement strategy to identify the engagement purpose, means by which engagement occurs or scenarios are managed, or the basis for there being more established information-sharing arrangements with some key stakeholders than with others. (See paragraphs 2.26 to 2.35)

12. The department's performance framework requires improvement. Critical infrastructure related content in the department's 2020–21 performance statements is not adequate. The department did not assess its critical infrastructure functions against the Regulator Performance Framework. The department has established internal performance reporting but could improve

its use of measures in the Critical Infrastructure Resilience Strategy to inform policy development and regulation. (See paragraphs 2.38 to 2.51)

Compliance activities

13. The department has established a compliance framework comprised of the Critical Infrastructure Resilience Strategy, Compliance Strategy and Administrative Guidelines. This framework would be enhanced by updating documents in the framework to align with and clarify the department's existing responsibilities and regulatory posture. (See paragraphs 3.2 to 3.7)

14. The majority of policy and procedural documents (15 of 22) to support possible critical infrastructure related compliance activities were drafted, but not finalised and approved, or included in the department's policy and procedural repository. A lack of procedures, or procedures that remain in draft, increases the risk of inconsistency in administration and decision-making. The department does not have an established process to ensure that appropriately trained officials are engaged in investigations under critical infrastructure regulations. Classified network and critical infrastructure-related system security controls do not meet the requirements to mitigate the risk of unauthorised access. (See paragraphs 3.10 to 3.20)

15. The department's use of regulatory tools is not always consistent with legislative and procedural requirements, and approved procedures or decision records do not exist for all compliance activities and outcomes. Use of regulatory tools was consistent with the department's documented regulatory posture. Decisions on whether to escalate to higher tiers of the regulatory compliance model were not supported by approved procedures, processes, or documented analysis of the administrative or financial burden associated with an escalation of compliance activity. (See paragraphs 3.23 to 3.29)

16. The department does not have an established process to obtain assurance of regulatory compliance. This limited the department's capacity to demonstrate that it has a proportionate and effective approach to resolving non-compliance, or has improved the security or resilience of critical infrastructure assets. (See paragraphs 3.30 to 3.44)

17. The department has not established a process to effectively review regulatory tool use, impacts on industry, or lessons learned to inform continuous improvement. (See paragraphs 3.45 to 3.46)

Recommendations

Recommendation no. 1 The Department of Home Affairs ensures that implementation of critical infrastructure related risk assessments and reporting is appropriate to inform policy and regulatory decisions.
Paragraph 2.24

Department of Home Affairs response: *Agreed.*

Recommendation no. 2 The Department of Home Affairs establish an engagement strategy to document how it will coordinate with stakeholders with shared responsibility for critical infrastructure security and resilience.
Paragraph 2.36

Department of Home Affairs response: *Agreed.*

Recommendation no. 3
Paragraph 2.52

The Department of Home Affairs ensure performance measurement:

- (a) in its corporate plan is adequate and measurable;
- (b) aligns with the Regulator Performance Guide; and
- (c) is used to inform policy and regulatory improvements.

Department of Home Affairs response: *Agreed.*

Recommendation no. 4
Paragraph 3.8

The Department of Home Affairs revise or replace the Critical Infrastructure Resilience Strategy with documentation that reflects current policy, regulatory responsibilities and posture, and outlines its application by the department in relation to other critical infrastructure asset sector policy leads and regulators.

Department of Home Affairs response: *Agreed.*

Recommendation no. 5
Paragraph 3.21

The Department of Home Affairs support effective use of the full suite of available critical infrastructure related regulatory tools by having in place procedures that:

- (a) are finalised, approved and lodged on the internal policy and procedural repository;
- (b) ensure that trained officials are appropriately engaged in investigations; and
- (c) align with the Protective Security Policy Framework and Information Security Manual requirements.

Department of Home Affairs response: *Agreed.*

Recommendation no. 6
Paragraph 3.39

The Department of Home Affairs approve, apply and monitor consistent use of policies, procedures and processes to:

- (a) trigger, triage and manage escalated use of critical infrastructure compliance powers, including by making better use of its information gathering, and investigatory powers where national security concerns have been identified; and
- (b) revise its risk approach and implement processes that enable effective assessment, prioritisation and management of non-compliance risks.

Department of Home Affairs response: *Agreed.*

- Recommendation no. 7** The Department of Home Affairs evaluate, monitor, and report on:
- Paragraph 3.47**
- (a) the extent to which regulatory tools are used to effectively improve security and resilience of critical infrastructure assets to risks; and
 - (b) implementation of actionable items in strategies, reviews and lessons learned for which it is responsible and how they contribute to intended outcomes.

Department of Home Affairs response: *Agreed.*

Summary of entity response

18. The department's summary response is provided below and its full response is included at Appendix 1. At Appendix 2, there is a summary of improvements that were observed by the ANAO during the course of the audit.

The Department of Home Affairs (the Department) accepts all of the ANAO's recommendations. Implementation of the 2021 and 2022 amendments to the *Security of Critical Infrastructure Act 2018* will be informed by ANAO's audit recommendations. The creation of the Cyber and Infrastructure Security Centre in the Department will bring together a coordinated all hazards approach to the protection of Australia's critical infrastructure. This will be undertaken both by direct regulatory responsibilities and in partnership with both industry, other Commonwealth regulators, as well as, state and territory governments.

Key messages from this audit for all Australian Government entities

19. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance and risk management

- Entities that do not have procedures, or have procedures that are inadequate or remain in draft, increase the risk of inconsistency in administration and decision-making.

Performance and impact measurement

- Entities should have performance measures that inform the Parliament of the achievement against regulatory and policy objectives. Performance measurement should be incorporated into an appropriate monitoring, reporting and evaluation framework.

Program implementation

- Compliance activities should be based on risk assessment and prioritisation, align with the severity and frequency of non-compliance, and escalate if the non-compliance is not rectified over time. Records should demonstrate that decisions align with the risks assessed, evidence, compliance framework and legislative powers.

Audit findings

1. Background

Introduction

1.1 Australian society and its economy are supported by a network of interconnected infrastructure assets across a broad range of industry sectors. The Australian Government defines critical infrastructure as:

those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly¹ impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.²

1.2 Threats such as natural disasters, pandemics, sabotage, and espionage have the potential to significantly disrupt critical infrastructure. Secure and resilient infrastructure ensures continuous access to services that are essential for everyday life, such as food, water, health, energy, communications, transport, and banking. A disruption to any of these critical infrastructure sectors could have serious implications for business, government, and the community.

1.3 The Commonwealth, state and territory governments have different responsibilities for critical infrastructure depending on the sector or nature of the threats being mitigated. Responses to a threat can involve the asset owner and operator, technical and operational lead for that jurisdiction, and emergency services or law enforcement. Coordination among entities is therefore required to prepare and respond to critical infrastructure threats.

1.4 The Department of Home Affairs (the department) is the lead Australian Government agency responsible for the administration of critical infrastructure policy and regulation.

Critical infrastructure policy and regulation

Regulatory options

1.5 Governments may approach regulation through either legislative or non-legislative models. Non-legislative models involve achieving regulatory ends through non-legislative means, such as guidelines on market participants³, and can include light touch or principles-based regulation⁴, self-regulation⁵ and quasi-regulation.⁶ Legislated approaches involve either

1 According to the Critical Infrastructure Centre Compliance Strategy 'In this context, "significantly" means an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia's international competitiveness in global markets, or impedes the continuity of government and its services.'

2 Australian Government, *Critical Infrastructure Resilience Strategy — Plan*, Attorney-General's Department, 2015, p.1.

3 Australian Government, *The Australian Government Guide to Regulatory Impact Analysis*, Department of the Prime Minister and Cabinet, 2020, p.30.

4 Where regulated entities are simply trusted to adhere to a framework of values and principles articulated in a code of conduct.

5 Where industry-written rules and codes of conduct are enforced by the industry itself.

6 Where rules or arrangements that are not part of explicit government regulation nevertheless seek to influence the behaviour of businesses, community organisations and individuals.

co-regulation⁷ or explicit government regulation, which is used where ‘there is a high perceived risk or public interest and achieving compliance is seen as critically important’.⁸

1.6 Australian Government regulators are empowered by, and subject to, a range of legal and other requirements including the following.

- Legislation that establishes the regulatory powers of an entity, and underpinning policies and relevant directions.
- The *Public Governance, Performance and Accountability Act 2013* along with delegated legislation such as the *Public Governance, Performance and Accountability Rule 2014*, the Commonwealth Procurement Rules, and the Commonwealth Risk Management Policy.
- The Australian Government Regulator Performance Framework — introduced in October 2014 — to encourage regulators to achieve their objectives while minimising their impact on regulated entities. On 1 July 2021, the Regulator Performance Guide⁹ replaced the 2014 Framework and included a transition year for regulators to assess their approach to complying with its requirements.

1.7 The Australian Government’s critical infrastructure regime is comprised of a combination of light touch, co-regulation and explicit government regulation.

Overview of the Australian Government critical infrastructure regime

1.8 Terrorist attacks in the United States in 2001, and Indonesia in 2002, were the catalyst for formal engagement between the Commonwealth, state and territory governments, and industry on how to prepare for and respond to threats against critical infrastructure assets. In 2003, the Australian Government established a Trusted Information Sharing Network as the primary engagement mechanism for business and government information sharing, and resilience building initiatives on critical infrastructure.

1.9 Prior to the introduction of critical infrastructure focussed policy and legislation in 2018¹⁰, national security threats to assets were primarily assessed under the *Foreign Investment and Takeovers Act 1975* (FATA). Under the FATA, certain proposed foreign investments, including those related to critical infrastructure assets require approval from the Treasurer. Conditions may be imposed, existing conditions may be varied, or a divestment from an approved investment may be required where a national security risk emerges.

1.10 The Treasury remains the lead entity for assessments under the FATA. The department provides national security advice to support decisions made under the FATA, and may impose and enforce conditions on approved applications. In 2020–21, the department received 943 applications for review from the Treasury, an increase from the 640 received during 2019–20.

7 A solution where industry develops and administers its own arrangements and the government provides the underpinning legislation to enforce it.

8 Australian Government, *The Australian Government Guide to Regulatory Impact Analysis*, Department of the Prime Minister and Cabinet, 2020, p.31.

9 Australian Government, *Regulator Performance Guide*, Department of the Prime Minister and Cabinet, 2021.

10 See paragraphs 1.14 to 1.21 below.

Critical Infrastructure Resilience Strategy

1.11 The Australian Government Critical Infrastructure Resilience Strategy was released in May 2015.¹¹ The strategy comprises a policy statement and plan, and sets out the Australian Government's policy position that:

- critical infrastructure is essential to Australia's economic and social prosperity;
- resilient critical infrastructure plays an essential role in supporting broader community and disaster resilience;
- businesses and governments have a shared responsibility for the resilience of critical infrastructure, requiring strong partnerships; and
- all states and territories have their own critical infrastructure programs that best fit the operating environments and arrangements in each jurisdiction.

1.12 The policy statement sets out an approach based on non-regulatory business–government partnerships, mature risk management, and effective information sharing. The policy statement required the strategy to be reviewed in 2020.

1.13 The Critical Infrastructure Centre was established in 2017 to coordinate the management of risks to Australia's critical infrastructure and deliver more coordinated national security assessments to inform foreign investment decisions in significant and complex cases. In December 2017, critical infrastructure policy, regulatory and strategy functions were transferred to the department and the Critical Infrastructure Centre became a division within the department.

Critical infrastructure legislation

1.14 In 2018, legislative coverage of the security of critical infrastructure expanded from the FATA to include:

- the *Security of Critical Infrastructure Act 2018* (SoCI Act), which commenced on 11 July 2018; and
- the amendments to Part 14 of the *Telecommunications Act 1997*, or Telecommunications Sector Security Reforms (TSSR), which commenced on 18 September 2018.

1.15 The legislation in paragraph 1.14 enables the government to obtain information to undertake risk assessments in relation to critical infrastructure, and gives government the power to issue directions to address national security risks if necessary.

Security of Critical Infrastructure Act 2018

1.16 The SoCI Act was introduced to 'strengthen the Government's capacity to manage the national security risks of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure'.¹² The SoCI Act defines a critical infrastructure asset¹³, and what

11 Australian Government, *Critical Infrastructure Resilience Strategy — Plan*, Attorney-General's Department, 2015.

12 Australian Government, *Security of Critical Infrastructure Bill 2017 Supplementary Explanatory Memorandum*, 2017, Australian Government p.2.

13 *ibid.*, subsection 9(1).

assets can¹⁴, and must not be prescribed as being ‘critical’.¹⁵ The SoCI Act has three measures to manage national security risks related to critical infrastructure.

- The Register of Critical Infrastructure Assets (the Register), provides the government visibility of who owns and controls the assets.¹⁶
- The information gathering power, provides the ability to obtain more detailed information from owners and operators of assets in certain circumstances.
- The Ministerial directions powers, provide the ability to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means.

1.17 In 2020, the Australian Government approved changes to the critical infrastructure regulatory regime on the basis that the SoCI Act did not enable it to impose requirements on entities to protect their assets, and an over-reliance on the FATA to manage risks arising from foreign ownership. In 2020, the department sought public contributions on the design of ‘an enhanced regulatory framework, building on existing requirements under the SoCI Act’.¹⁷

1.18 In December 2020, the Australian Government introduced a Bill that included amendments to the SoCI Act. These amendments would enact the regulatory framework that was the subject of public consultation. The Bill proposed mandatory incident reporting, an expanded application of the register of critical infrastructure sectors and assets, powers to obtain ownership, operational and risk management information, and powers to respond to serious cyber incidents. The amendments to the SoCI Act were described when they were introduced, as being ‘underpinned by enhancements to Government’s existing education, communication and engagement activities, under a refreshed Critical Infrastructure Resilience Strategy’.¹⁸

1.19 In December 2020, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) commenced an inquiry into the Bill that would amend the SoCI Act, as well as a statutory review into the Act.¹⁹ In September 2021 the PJCIS published an Advisory Report on the concurrent reviews of the Bill and statutory review of the SoCI Act and made 14 recommendations. Among

14 *ibid.*, subsection 9(2).

15 *ibid.*, section 9, subsections 3 and 4.

16 Australian Government, *2019–20 Annual Report*, Department of Home Affairs, 2020, p. 47, available from <https://www.homeaffairs.gov.au/reports-and-pubs/Annualreports/home-affairs-annual-report-2019-20.pdf> [accessed 5 January 2022].

The department’s 2019–20 Annual Report states that 167 entities were listed on the Register.

17 Australian Government, *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper August 2020*, 2020, Australian Government, p.4.

18 Australian Government, *Security Legislation Amendment (Critical Infrastructure) Bill 2020 Explanatory Memorandum*, 2020, Australian Government, p.3.

19 Australian Parliament House, *Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*, APH, 2021, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/SOCI [accessed on 30 November 2021].

the recommendations was that the Bill be split in two so that government assistance²⁰ and an expanded definition of critical infrastructure sectors and assets could be legislated in the shortest time possible.

1.20 An additional \$42.4 million over two years from 2021–22²¹ was included in the 2021–22 Budget for ‘Protecting Critical Infrastructure and Systems of National Significance’.

- In September 2021, the Critical Infrastructure Centre was re-branded as the Cyber and Infrastructure Security Centre.
- In December 2021, amendments to the SoCI Act expanded the asset classes covered from four to 22 across 11 sectors to include: communications, financial services and markets, data storage and processing, defence industry, higher education and research, energy, food and grocery, health care and medical, space technology, transport, and water and sewerage.²² The department estimated that it would have ten times the number of assets on its Register under the SoCI Act as a result of this change.
- Also in December 2021, the Australian Government commenced consultations on further amendments to the SoCI Act.²³
- In March 2022, the PJCIS published an Advisory Report on the proposed further amendments to the SoCI Act and made 11 recommendations.²⁴

1.21 In March 2022, the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* was passed by the Parliament. Details of changes to Australian Government critical infrastructure legislation are in Appendix 3.

Telecommunications Sector Security Reforms

1.22 The TSSR established a regulatory framework ‘to better manage the national security risks of espionage, sabotage and foreign interference to Australia’s telecommunications networks and facilities’.²⁵ The purpose of the TSSR is to:

20 Departmental guidance states that the:

Government Assistance framework provides the Minister for Home Affairs with the ability to authorise the Secretary of the department to do any or all of the following things in response to a cyber security incident: gather information to determine if another power in the [SoCI Act] should be exercised; direct an entity to do, or refrain from doing, a specified act or thing; request an authorised agency ... to provide support (with agreement from the Prime Minister and Minister for Defence).

Department of Home Affairs, *Cyber Incident Response Government Assistance Measures*, DHA, 2022, available from <https://www.cisc.gov.au/critical-infrastructure-centre-subsite/Files/cyber-incident-response-government-assistance-measures.pdf> [accessed on 31 March 2022].

21 2021–22 Department of Home Affairs Portfolio Budget Statements refers to an allocation of \$23.9 million in 2021–22 and \$18.5 million in 2022–23.

22 These amendments to the SoCI Act were made under the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2021*.

23 Department of Home Affairs, *Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (SLACIP Bill)*, DHA, 2022.

24 Parliament of Australia, *Advisory report on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022*, APH, 2022.

25 Department of Home Affairs, *Telecommunications Sector Security Reforms* [internet], DHA, available from <https://www.homeaffairs.gov.au/nat-security/Pages/telecommunications-sector-security-reforms.aspx> [accessed on 30 November 2021].

- introduce a comprehensive risk-based regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities; and
- better protect networks, and the confidential information stored on and carried across them, from unauthorised interference and access.

1.23 The aim of the TSSR is to encourage early engagement on proposed changes to networks and services that could give rise to national security risks, and to facilitate collaboration on the management of those risks. Key elements of the TSSR include:

- a security obligation that requires all carriers, carriage service providers and carriage service intermediaries to do their best to protect networks and facilities from unauthorised access or interference²⁶;
- a notification obligation that requires carriers and nominated carriage service providers to notify the Australian Government of planned changes to their networks and services that are likely to have a material adverse effect on their capacity to comply with the security obligation;
- that the Secretary of the department can obtain information and documents for the purpose of assessing carriers and carriage service providers compliance with their security obligations; and
- that the Minister for Home Affairs can direct a carrier, carriage service provider or carriage service intermediary to:
 - not use or supply carriage services if the Minister considers the use or supply prejudicial to national security; and
 - do, or not do, a specified thing that is reasonably necessary to protect networks and facilities from national security risks.

1.24 In September 2020, the PJCIS commenced a statutory review of the operation of the TSSR.²⁷ The PJCIS published its report on the statutory review in February 2022 and made six recommendations.²⁸

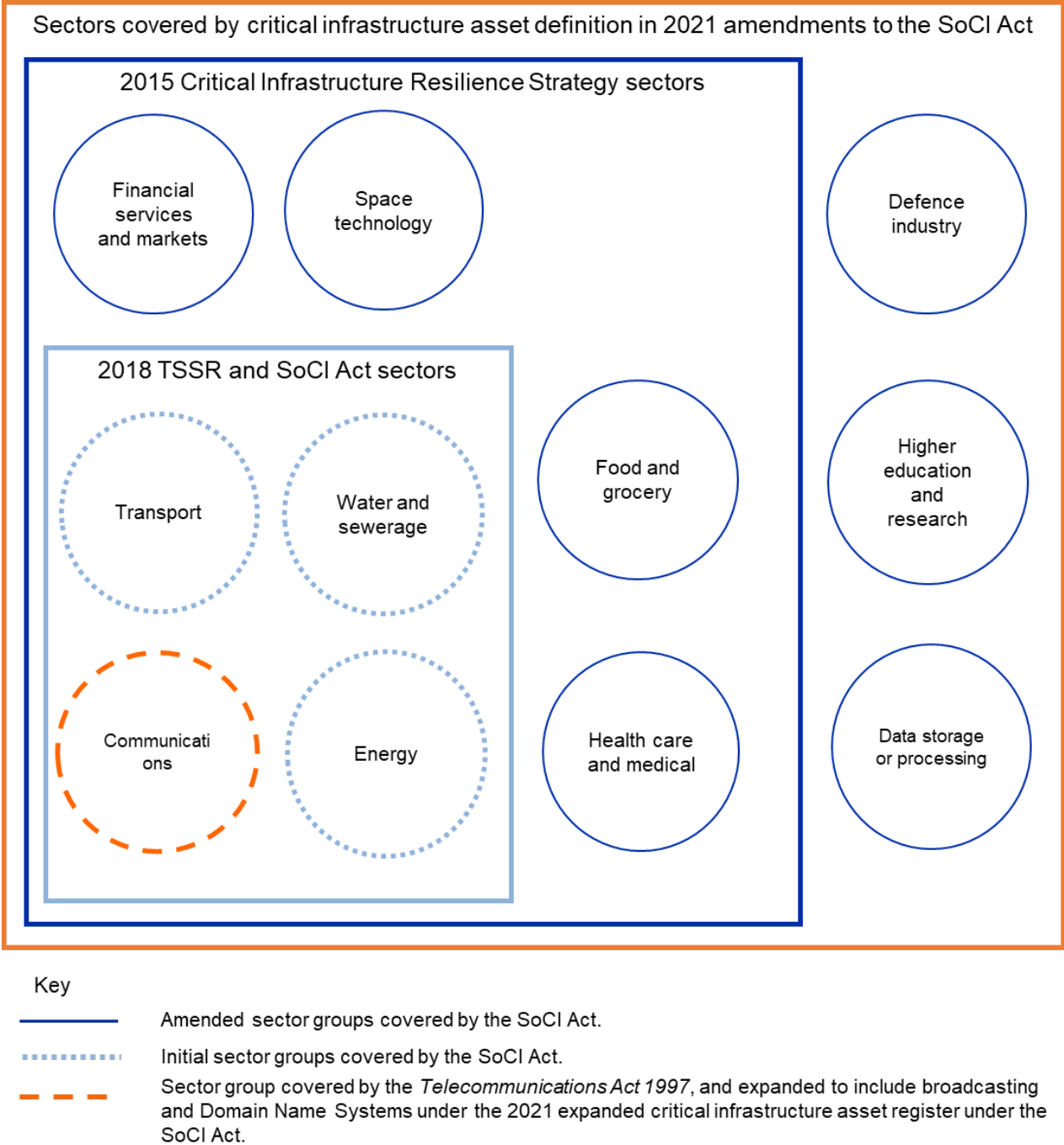
1.25 Figure 1.1 illustrates the sectors covered by Australian Government critical infrastructure policy and legislation.

26 Telecommunications Act, section 311.

27 Parliament of Australia, *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms* [Internet], APH, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Part14Telecommunication [accessed on 30 November 2021].

28 *ibid.*

Figure 1.1: Australian Government critical infrastructure policy and legislation sector coverage



Note: Sectors illustrated in the figure as being relevant to particular legislation may not represent all asset classes within them. For example, while the transport sector consists of public transport, aviation, maritime ports, freight infrastructure, and freight services, only specific maritime ports were captured under the 2018 SoCI Act and may be subject to an expanded number of transport asset types under the register following 2021 amendments to the SoCI Act.

Source: ANAO analysis of departmental documentation.

Critical infrastructure security and resilience roles

1.26 The Commonwealth, state and territory governments, and industry, have a shared responsibility to ensure the security and resilience of critical infrastructure, and to prevent, prepare,

respond to, and recover from all hazards. Each participant has different roles as shown in Table 1.1. Further detail of the entities involved, and key policies and legislation is in Appendix 3.

Table 1.1: Critical infrastructure roles

Role	Commonwealth	States and territories	Industry
Policy lead	✓	✓	✗
Service provider	✓ ^a	✓ ^b	✓
Operational lead	✓	✓	✓
Regulator	✓	✓	✗
Owner/Operator	✓	✓	✓

Key: ✓ = role exists.

✗ = role does not exist.

Note a: For example, weather forecasting and cyber protection advisory notice provision.

Note b: For example, managing threats to life and property, preparing, and responding to emergencies, ensuring law and order, and delivery services such as health care and water.

Source: ANAO analysis of departmental documentation.

1.27 The department, as the lead agency for ensuring the protection of critical infrastructure, must coordinate, complement, and support the programs and activities of all these participants. When the Critical Infrastructure Centre and SoCI Act were established, it was recognised that the Australian Government would have limited powers to implement risk management strategies, and monitor and enforce compliance, and should first leverage existing state and territory regimes to conduct these activities.

Rationale for undertaking the audit

1.28 The potential for an attack²⁹ that degrades or disables a critical infrastructure asset has been identified by industry and governments in Australia and abroad. This audit provides assurance to the Parliament on whether the department, as policy and regulatory lead for critical infrastructure protection coordination, has an effective approach to protecting Australia's assets of national significance, and supporting asset owners and operators to improve their resilience to attacks.

Audit approach

Audit objective, criteria and scope

1.29 The audit objective was to assess the effectiveness of the department's administration and regulation of critical infrastructure protection policy. To form a conclusion against this objective, the following high-level criteria were applied.

²⁹ Australian Government, *Cyber Security Strategy 2020*, DHA, 2020, available from <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>.

The document noted that critical infrastructure providers were the victims of around 35 per cent of reported cyber incidents perpetrated by malicious actors in the year to 30 June 2020.

- Has the department established effective governance arrangements to administer critical infrastructure protection policy?
- Does the department effectively administer compliance activities consistent with critical infrastructure protection requirements?

Audit methodology

1.30 The following actions were done to address the audit objective.

- The audit team examined departmental documentation with a focus on:
 - risk inputs, including systems and review of risk ratings and products;
 - processes, procedures, guidance and documentation developed to support, or as a result of, compliance activities;
 - departmental data used to inform reporting on compliance activities; and
 - arrangements with partner agencies.
- The audit team undertook system mapping and control testing over key systems, including a review of departmental assurance over the quality and integrity of inputs from other entities.
- The audit team undertook case studies into instances of non-compliance involving the use of enforcement activities.
- The audit team conducted meetings with relevant departmental staff and stakeholders.

1.31 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately \$349,000.

1.32 The team members for this audit were Glen Ewers, Rebecca Helgeby, Jessica Kanikula, Edwin Apoderado, Ji Young Kim, and Alex Wilkinson.

2. Governance arrangements

Areas examined

This chapter examines whether the Department of Home Affairs has effective governance arrangements to administer critical infrastructure protection policy, including risk identification and management, stakeholder engagement and an appropriate performance framework.

Conclusion

The department has partly effective governance arrangements to administer critical infrastructure protection policy. Implementation of critical infrastructure related risk assessments and reporting was not captured in risk documentation. The effectiveness of the department's stakeholder coordination arrangements is reduced by not having an engagement strategy and providing limited support to other critical infrastructure regulators. The department's performance framework as it related to critical infrastructure was not adequate, with performance statements, regulatory performance assessment, and use of internal measures to inform policy and regulation requiring improvement.

Areas for improvement

The ANAO made three recommendations aimed at the use of risk management to inform decision-making, establishing an engagement strategy, and having appropriate performance measurement.

2.1 Critical infrastructure policy, regulatory and strategy functions have been the responsibility of the Department of Home Affairs (the department) since December 2017. The Australian Government's Critical Infrastructure Resilience Strategy³⁰ outlines how the department will support asset owners and operators to effectively manage reasonably foreseeable and unforeseeable risks to the continuity of their operations.

2.2 Implementation of the government's critical infrastructure policy objectives requires effective governance arrangements that reflect the risk environment, and the importance of coordination between the different levels of government and asset owners. To assess the extent to which the department had effective governance arrangements to administer critical infrastructure protection policy, the ANAO examined the material components of the department's critical infrastructure related governance arrangements, which comprise its risk identification and management processes, stakeholder engagement coordination, and performance framework.

Are risks to critical infrastructure assets identified and managed effectively?

The department identified key critical infrastructure risks and had appropriate governance arrangements to assess and assign responsibility for these risks. The department's critical infrastructure risk management does not represent an integrated approach to risk management between its enterprise and operational, legislative and policy functions. Implementation of critical infrastructure related risk assessments and reporting was not

30 Australian Government (2015), *Critical Infrastructure Resilience Strategy— Policy Statement*, Attorney-General's Department, 2015, p.7.

captured in risk documentation, which reduces its use to inform business planning, legislative reform, and policy decisions.

2.3 Regulators with clear and comprehensive processes to assess risk are positioned to allocate their resources towards those areas of greatest impact. The department's enterprise risk management framework aims to fully integrate risk management in planning and decision-making activities. Critical infrastructure risk is addressed by the department through:

- enterprise level risks;
- business area annual planning;
- informing draft legislation to address national security risks associated with Australia's critical infrastructure; and
- critical infrastructure protection coordination in the:
 - provision of advice to the Treasury on foreign investment and acquisition applications; and
 - engagement with the critical infrastructure industry and government stakeholders to support and understand asset resilience and incident response.

Enterprise level

Assessment and reporting alignment

2.4 In 2020–21, the department identified and assessed three enterprise level risks that addressed critical infrastructure.³¹ The main enterprise risk is 'critical infrastructure', which is '[a]n attack on critical infrastructure [that] significantly disrupts national operations, causing damage to the economy, public safety, and national security.'³² The other two enterprise risks address cyber and disasters.

2.5 Enterprise risk governance arrangements include reporting to the following internal governance forums:

- annual updates and a dashboard of all enterprise risks to the Executive Committee;
- quarterly updates and a dashboard, and three detailed reviews to the Enterprise Operations Committee and the Risk Committee; and
- enterprise risk update as a standing item for the department Audit and Risk Committee.

2.6 In 2020–21, reporting on enterprise risks and controls provided the accountable authority with visibility of critical infrastructure enterprise risks, and was consistent with the arrangements outlined above in paragraph 2.5.

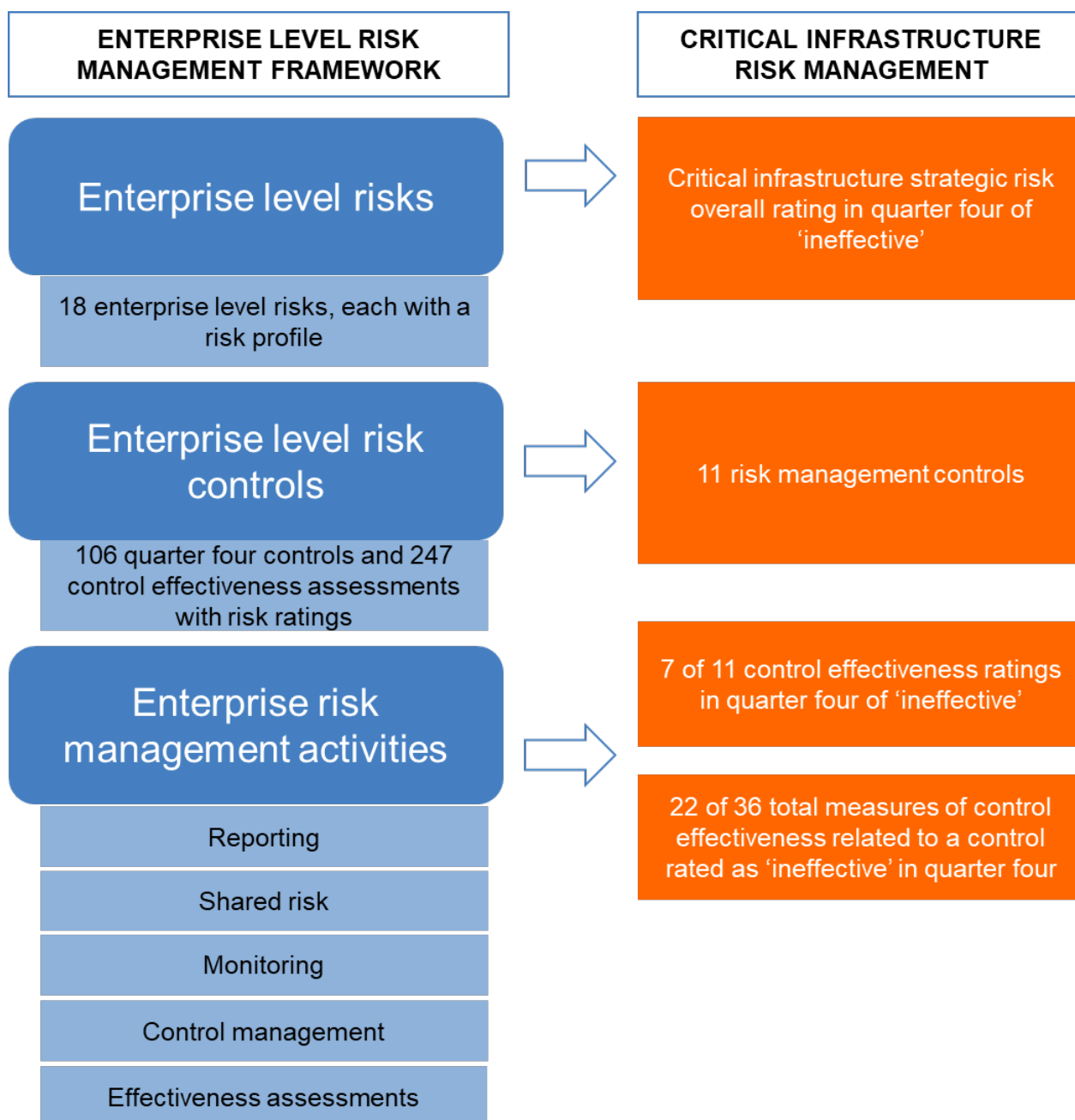
2.7 Updates to the department's Audit and Risk Committee on enterprise level risks included information on risk ratings, threats, consequences, related risks, the effectiveness of controls, and collaboration with key stakeholders. Each enterprise risk is assigned a risk owner. Controls for each risk are rated according to their effectiveness at mitigating the risk after the control has been applied. These 'control effectiveness ratings' are also included in quarterly reporting, and represent the last assessed performance of the control. Figure 2.1 illustrates key components of the

31 In 2020–21, the department had 18 enterprise level risks.

32 Department of Home Affairs, *2020–2021 Corporate Plan*, DHA, 2020, p.25.

department's enterprise level risk management framework and how it has been applied to its critical infrastructure risk.

Figure 2.1: The department's enterprise risk management framework and critical infrastructure strategic risk management in 2020–21



Source: ANAO analysis of departmental documentation.

2.8 In November 2021, the Executive Committee requested that quarter four reporting be reviewed to ensure it presents an accurate and realistic picture, and the outcomes of the review are reported to the Secretary. Subsequently, revisions made to the critical infrastructure enterprise risk report took the number of ineffective control ratings for the enterprise level critical

infrastructure risk from one to seven of the eleven ratings³³, and the critical infrastructure risk was rated as ineffective.³⁴

2.9 While the department had identified the risk to critical infrastructure at the enterprise level, supporting documentation did not effectively address the risk.

- Controls did not align with activities or risk ratings listed against them.³⁵
- There was no reporting against the 36 measures of control effectiveness in each quarter, or for the reporting period.
- Most of the 11 control effectiveness ratings were inconsistent with the rating matrix in the Strategic and Enterprise Risk Management Plan and Reporting Handbook and not substantiated by reporting against each control.

2.10 Risk information submitted to governance bodies is dependent on the quality and maintenance of information included in risk reporting. Inconsistent and unsubstantiated content in risk reports reduces the department's effectiveness in informing critical infrastructure related policy, or regulatory decisions.

Shared risk

2.11 The Commonwealth, state and territory governments, and industry have a shared responsibility to address the risks to critical infrastructure.³⁶ The *Commonwealth Risk Management Policy* requires the department to implement arrangements to understand and contribute to the management of shared risks.³⁷ The department's risk management framework considers shared risks to include:

- ensuring visibility of risk through proactive information exchange;
- designing, deploying, and monitoring and reporting effectiveness of controls and risk treatments; and
- establishing mechanisms to share the burden of risk when it is realised.

2.12 The department's processes for addressing the shared risk relating to critical infrastructure did not include a number of aspects of its risk framework. Internal reporting for quarter four 2020–21 addressing the critical infrastructure enterprise level risk:

- identified only two operational stakeholders as external shared risk owners;
- contained no reference to state or territory governments, or other operational and regulatory bodies; and

33 At the enterprise level, the critical infrastructure enterprise risk accounted for seven of nine ineffective control ratings out of a total of 247.

34 This was the first enterprise level risk assessed as ineffective since 2018.

35 For example, the 'engagement' control includes an activity of 'consistent participation and informative, outcomes based discussion forums across stakeholders', and yet reporting for the control does not refer to whether participation in forms of engagement were consistent, whether discussions focused on or led to outcomes or measured the extent of stakeholder coverage. Reporting does not justify why the control is rated as 'partially effective'. Of the 36 control measures, 28 did not align with reported activities and ratings.

36 See paragraph 1.26. Effective coordination of risk between stakeholders is addressed below in paragraphs 2.26 to 2.35.

37 Department of Finance, *Commonwealth Risk Management Policy*, DoF, 2014, p.16.

- referred to the department having limited visibility of information held by one of the shared risk owners as a basis for assessing the overall risk rating for the critical infrastructure enterprise level risk as ineffective.

2.13 Engagement in different fora and with specific stakeholders to achieve departmental objectives is referred to in enterprise level critical infrastructure related risk assessments. Critical infrastructure related risk reporting also refers to activities that assess or manage shared risks. Reporting that relates to critical infrastructure regulatory or policy responsibilities is limited to legislative and policy reform, and foreign investment and acquisition assessments, and excludes:

- other Australian Government regulatory bodies in critical infrastructure sectors;
- state and territory government agencies with critical infrastructure policy, operational or regulatory responsibilities; and
- critical infrastructure asset owners and operators.

Business planning

2.14 Management of risk at the operational level should effectively integrate with the enterprise level risk framework. The Cyber and Infrastructure Security Centre (CISC) of the department is responsible for the administration and regulation of critical infrastructure policy. The 2020–21 and 2021–22 business plans for the CISC³⁸ included:

- key risks that aligned with enterprise level critical infrastructure strategic risk documentation; and
- controls that aligned with the enterprise level critical infrastructure risk.

2.15 Management meetings were used to progress business plan outputs and did not consider the impact activities were having on mitigating identified risks.

Advice on the legislative framework

2.16 The department's risk framework should inform its policy advice related to critical infrastructure regulation. The *Security of Critical Infrastructure Act 2018* (SoCI Act) is designed to manage national security risks arising from foreign involvement in Australia's critical infrastructure. It initially covered the electricity, gas, water, and ports sectors on the basis that the degradation or disruption of assets in these sectors was most likely to have a negative impact on the Australian economy or security.

2.17 The department is also required under the Telecommunications Security Sector Reforms (TSSR) to assess national security risks to critical telecommunications infrastructure arising from proposed changes notified by providers (use of these powers is discussed further in chapter 3, paragraphs 3.23 to 3.29). The department has provided advice and reported on the use of regulatory powers under the SoCI Act and TSSR. The assessed risks and advice did not result in adjustments to critical infrastructure risk assessment at the enterprise level, in business planning or in any other risk assessment.

³⁸ The 2020–21 business plan was established prior to the Critical Infrastructure Centre being re-branded as the Cyber and Infrastructure Security Centre (see paragraph 1.20).

Policy lead activities

2.18 The department has adopted a risk-based approach to prioritising compliance activities and allocating resources under both the SoCI Act and the TSSR (see paragraphs 3.31 and 3.32). Activities conducted under the compliance model did not result in adjustments to enterprise or business plan risk assessments and ratings based on the outcome of these activities. Outcomes of these activities were not integrated into the enterprise level critical infrastructure strategic risk summary reporting, or its supporting documentation.

2.19 Under the *Foreign Investment and Takeovers Act 1975* (FATA) arrangements, the department is required to support the management of risk to critical assets. The department provides advice on foreign investment and acquisition applications. Departmental advice is based on the application of a risk assessment procedure, which supports the consistent assessment of the threat, vulnerability, and consequences of what was proposed in the applications, to the continued operation of critical infrastructure assets and services.

2.20 A review of a sample of FATA assessments by the ANAO found that the department was consistent with its procedural requirements. The department also provided advice, through the Foreign Investment Strategic Analysis Team, on national security risks associated with applications.

2.21 Advice provided by the department on critical infrastructure risks included in individual foreign investment assessments was not used to inform adjustments to overall assessments of related enterprise risks or the effectiveness of controls. For example, reporting provided to the governance forums outlined above in paragraph 2.5 on the critical infrastructure enterprise risk, did not reflect intelligence gained from individual foreign investment assessments, or trends that would inform the management of potential national security concerns.

2.22 The 2015 Critical Infrastructure Resilience Strategy includes two core policy objectives that relate to the department's role in overseeing industry risk management. These are for critical infrastructure owners and operators to be effective in managing:

- reasonably foreseeable risks to the continuity of their operations, through a mature, risk-based approach; and
- unforeseen risks to the continuity of their operations through an organisational resilience approach.³⁹

2.23 The department provides the Organisational Resilience Health Check on its website⁴⁰ as a tool for industry to self-assess organisational resilience capability. Responses are confidential and are not recorded by the department. The tool is not referred to in any enterprise risk documentation as a means by which threat preparedness or responsiveness could be improved. Use of the health check is not monitored by the business area responsible for critical infrastructure.

39 Australian Government, *Critical Infrastructure Resilience Strategy — Plan*, Attorney-General's Department, 2015, p.1.

40 Department of Home Affairs, *HealthCheck* [Internet], DHA, 2020, available from <https://www.organisationalresilience.gov.au/HealthCheck/overview> [accessed 9 February 2022].

Recommendation no. 1

2.24 The Department of Home Affairs ensures that implementation of critical infrastructure related risk assessments and reporting is appropriate to inform policy and regulatory decisions.

Department of Home Affairs response: *Agreed.*

2.25 *The department agrees to recommendation 1 of the report. The establishment of the Cyber and Infrastructure Security Centre (CISC) on 1 September 2021 has brought together the critical infrastructure regulatory and security risk assessment functions of the department. The CISC continues to enhance its risk assessment framework to support regulatory and policy decisions with a view to capabilities to all 11 critical infrastructure sectors — following passage of the Security Legislation Amendment (Critical Infrastructure) Act 2021.*

Have effective coordination arrangements with key stakeholders been established?

While the department undertakes coordination activities with key stakeholders, including through some long-established forums, it does not have a documented stakeholder engagement strategy to identify the engagement purpose, means by which engagement occurs or scenarios are managed, or the basis for there being more established information-sharing arrangements with some key stakeholders than with others.

2.26 The department's management of critical infrastructure protection relies on coordination with other Commonwealth entities, state and territory governments, asset owners and operators (see paragraph 1.26). The 2015 Critical Infrastructure Resilience Strategy includes the following Australian Government policy positions:

- businesses and governments have a shared responsibility for the resilience of our critical infrastructure, requiring strong partnerships; and
- all states and territories have their own critical infrastructure programs that best fit the operating environments and arrangements in each jurisdiction.

2.27 The department has stated that the update⁴¹ to the 2015 Critical Infrastructure Resilience Strategy will:

- bring disparate work across government together. This helps create a consistent approach to improving critical infrastructure security and resilience. It will give holistic support to owners and operators across the threat spectrum; and
- provide a framework for how we work with state and territory governments and industry.⁴²

41 The Strategy states that '[t]o ensure the Australian Government's policy settings remain appropriate, the Strategy will undergo a comprehensive review in 2020...'

Australian Government, *Critical Infrastructure Resilience Strategy — Policy Statement*, Attorney-General's Department, 2015, p.13.

42 Australian Government, *Critical Infrastructure Resilience Strategy* [Internet], DHA, 2021, available from <https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy> [accessed 9 February 2022].

Engagement approach

2.28 The department does not have an engagement strategy in place for critical infrastructure that identifies the purpose and means for engagement, relevant stakeholders, or distinguishes when the department is undertaking a policy or regulatory role. Sector specific strategies were developed for four sectors to inform engagement on legislative reforms. These strategies were discontinued before the reform engagement had concluded and replaced with an engagement approach that was not industry specific. The sector specific strategies did not relate to the department's engagement on its legislated regulatory functions.

2.29 The department participates in key forums to engage with government and industry stakeholders listed in Table 2.1.

Table 2.1: Summary descriptions of key critical infrastructure-related engagement

Forum	Summary description
Critical Infrastructure Advisory Council (CIAC)	The CIAC is responsible for leadership and setting the strategic direction for the Trusted Information Sharing Network (TISN). Participants include select TISN members (sector chairs), states and territories and Australian Government representatives and meetings are used to discuss critical infrastructure issues. CIAC meeting frequency has been inconsistent, and since 2017 has ranged from meetings occurring 18 months apart to being held monthly.
TISN sector groups	Established in 2003, the TISN comprises eight sector-based groups that cover the following critical infrastructure sectors: water services; energy; banking and finance; food and grocery; communications; health; transport; and Commonwealth. Meeting frequency has been inconsistent for each sector group. One sector group had not met for two years and had a Terms of Reference dated 2013, while others met on a monthly basis.
All Hazards Community of Interest	These meetings are co-chaired by Emergency Management Australia and the CISC on a weekly basis, and cover common and shared hazards, such as bushfires and weather events. The meetings are open to all TISN members and provide a forum for government and industry to exchange information and discuss pressing critical infrastructure issues.
Taskforce meetings	Meetings are held as required, to discuss specific threats that warrant a coordinated response. For example, the Supermarket Taskforce, whose members include representatives from states and territories, senior government executives and industry sector members, met to discuss challenges of the COVID-19 pandemic. Also, the Bushfire Taskforce met in response to threats from bushfires in the summer of 2019–20. While these meetings were not specifically about critical infrastructure assets, they did include items related to them.
Legislative and policy reform meetings	In 2020–21, the department completed public and targeted stakeholder consultation on the development of amendments to the SoCI Act, the next Critical Infrastructure Resilience Strategy, and an updated TISN. On the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (SoCI Bill), consultation included the release of discussion papers and an exposure draft, workshops and bilateral meetings. 'These consultation processes were intended to guide the development of the framework proposed in the SoCI Bill, essentially being the first step in the co-design process at the foundation of the regulation'.

Forum	Summary description
Bilateral engagement	Official level bilateral engagement occurred between the department and stakeholders with policy, operational or regulatory responsibilities in critical infrastructure sectors.

Source: ANAO analysis of departmental documentation.

2.30 The engagements listed in Table 2.1 focussed on sharing information on issues such as cyber, natural hazard forecasting, and supply chain updates. The meetings did not provide a strategic approach to ensuring critical infrastructure policy outcomes were met, or provide a platform for the sharing of better practice, setting sector expectations, or distributing information to assist other Australian Government, state or territory critical infrastructure regulators to pursue possible instances of non-compliance under their regulatory powers. While components of existing policy and forum terms of reference covered some aspects of the department's critical infrastructure related responsibilities, they did not represent an engagement strategy that comprehensively covers:

- when engagement is in a policy or regulatory capacity;
- how the department will support other regulatory bodies and industry to improve critical infrastructure resilience and security; or
- information sharing arrangements with relevant regulatory bodies.

2.31 The CIAC and seven of eight TISN sector groups have terms of reference that align with the matters covered in meetings held since 2017. In 2021, a TISN online platform was established, and membership reset to align with the expanded sectors covered under the SoCI Act. The TISN was described as still being a forum for the department to engage in a non-regulatory capacity with:

stakeholders from across the critical infrastructure community, including critical infrastructure owners and operators, supply chain entities, peak bodies, industry specialists and all levels of government who are responding to the increasingly interconnected and interdependent nature of Australia's critical infrastructure.⁴³

2.32 In addition to the forums listed in Table 2.1, the department engages on an as needed basis with other regulators, particularly with the:

- Treasury to provide advice on the national security implications of applications made under the FATA; and
- Australian Communications and Media Authority about the issuing of carrier licences that requires approval from the Communications Access Coordinator (CAC)⁴⁴ under the TSSR.

Information sharing

2.33 Effective communication arrangements ensure agencies receive information they need to undertake their functions. It also enables agencies to coordinate with, and benefit from, activities undertaken by other agencies. The SoCI Act allows the department to share information that it has

43 Department of Home Affairs, *Unpublished: Trusted Information Sharing Network (TISN) Online Engagement Platform*, DHA, p.1.

44 This role is specified in the *Telecommunications (Interception and Access) Act 1979* and can be the Secretary of the department, or a person or body specified by the Minister. The action of the CAC is taken to be on behalf of all the interception agencies and all the enforcement agencies. The CAC liaises between security and law enforcement agencies and the telecommunications industry.

obtained with relevant entities responsible for the regulation, or oversight of critical infrastructure assets.⁴⁵

2.34 Regulatory and non-regulatory arrangements apply to the collection of information by the department relating to critical infrastructure. Under the SoCI Act, asset owners have an obligation to report specific information to the department's Register of Critical Infrastructure Assets. Under the TSSR, entities that are carriers and nominated carriage service providers may advise of changes with potential security risks.⁴⁶

2.35 Other Commonwealth, state and territory regulators obtain critical infrastructure asset information under their respective functions (see Appendix 4). The department does not use arrangements in Table 2.1 to obtain or share threat prevention and preparedness related information with these regulators.⁴⁷ While the department informed the ANAO it shares information with states and territories, and other Australian Government regulatory bodies, the ANAO did not identify a consistent or risk-based approach. Consequently, more established information-sharing arrangements exist with some key stakeholders⁴⁸ and not others.⁴⁹

45 *Security of Critical Infrastructure Act 2018*, section 42.

46 *Telecommunications Act 1997*, sections 314A and 314C.

47 In this context, other Commonwealth regulators include the: Australian Communications and Media Authority, Treasury and Treasurer, Australia Energy Regulator, Australian Energy Market Commission, and the National Offshore Petroleum Safety and Environmental Management Authority.

48 Such as the Treasury, the Australian Security Intelligence Organisation, the Australian Communications and Media Authority and the Independent Pricing and Regulatory Tribunal in New South Wales.

49 Key stakeholders not referred to in footnote 48 are listed in Appendix 4.

Recommendation no. 2

2.36 The Department of Home Affairs establish an engagement strategy to document how it will coordinate with stakeholders with shared responsibility for critical infrastructure security and resilience.

Department of Home Affairs response: *Agreed.*

2.37 *The department agrees to recommendation 2 of the report. As noted by the ANAO, the department produced sector-specific engagement strategies in 2021 and will do so in 2022 focused on the legislative reforms and how best to support sectors through the reforms journey. Following the passage of both tranches of the reforms, the CISC has released “Protecting Australia Together” which outlines CISC functions, mission and approach to provide an understanding to industry on the way our work will enable all facets of the critical infrastructure community to remain secure and resilient, for the benefit of all. “Protecting Australia Together” will be supported by the release of Stakeholder Communication and Engagement Strategy which documents, in a specific and tangible way, how CISC will coordinate the shared responsibility for critical infrastructure security and resilience with all 11 critical infrastructure sectors. The department agrees that there is an ongoing need to ensure clarity of responsibility and accountability for ensuring steps are taken to maintain security of Australia’s critical infrastructure. The portfolio is aligned with the requirements under the Regulator Performance Guide, which came into effect from 1 July 2021. To date, the Portfolio has been provided Ministerial Statements of Expectations for all its regulatory functions, including the CISC, and is progressing a corresponding Statements of Intents. This will demonstrate the strong commitment to meeting stakeholder expectations while delivering the Government’s policy priorities and supporting the regulatory reform agenda. An integral part of this will be clear articulation of how the Portfolio regulators will engage with industry and continue to strive for continuous improvement. Both the Statement of Expectations and Statement of Intents will be publicly available in due course. Refer also to the response to recommendation 4, as the Critical Infrastructure Resilience Strategy will contribute towards achieving this recommendation.*

Has an effective performance framework been established?

The department’s performance framework requires improvement. Critical infrastructure related content in the department’s 2020–21 performance statements is not adequate. The department did not assess its critical infrastructure functions against the Regulator Performance Framework. The department has established internal performance reporting but could improve its use of measures in the Critical Infrastructure Resilience Strategy to inform policy development and regulation.

2.38 A key element of regulatory governance is the establishment of an appropriate performance framework that provides information about whether the regulator is achieving its intended results. This should include external performance measures to provide information about the achievement of its purpose to the Parliament and other stakeholders, and internal performance measures to inform officials about the efficiency, effectiveness, economy and ethics of their regulatory and policy approach.

Performance framework

Performance measure adequacy

2.39 Under the Commonwealth Performance Framework, an entity must report on how its performance in achieving its purposes and key activities will be measured and assessed.⁵⁰ To provide accountability to the Parliament and the public, the results against these measures are required to be provided in annual performance statements.⁵¹

2.40 In 2020–21 and 2021–22, the performance measure relating to critical infrastructure contained in department's Portfolio Budget Statements and corporate plan were broadly consistent.

- The department's 2020–21 and 2021–22 Portfolio Budget Statements each included a single program, purpose and performance measure, with one target that relates to its critical infrastructure responsibilities.
- The department's 2020–21 and 2021–22 corporate plans each included three purposes, with critical infrastructure responsibilities falling under purpose 1 on national security.⁵² The 2020–21 corporate plan also stated that 'ownership of critical infrastructure must continue to be managed and resilience will need to be enhanced to ensure it cannot be compromised by natural hazards, organised criminals, or foreign actors'.⁵³
- The 2020–21 and 2021–22 corporate plans each include one key activity, one composite measure and four targets that related to the department's critical infrastructure responsibilities.

2.41 The ANAO assessed the department's 2020–21 critical infrastructure performance measure against the requirements of the Commonwealth Performance Framework and accompanying guidance.⁵⁴ The ANAO did not assess the appropriateness of the department's entity-wide set of performance measures, and reviewed only the measure directly relating to the critical infrastructure program.

2.42 Section 16EA of the *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule) requires an entity's performance measures, in the context of the entity's purposes or key activities, to:

- (a) relate directly to one or more of those purposes or key activities;
- (b) use sources of information and methodologies that are reliable and verifiable;
- (c) provide an unbiased basis for the measurement and assessment of the entity's performance;

50 The Commonwealth Performance Framework consists of the *Public Governance, Performance and Accountability Act 2013*, the *Public Governance, Performance and Accountability Rule 2014* and accompanying guidance issued by the Department of Finance.

51 *Public Governance, Performance and Accountability Rule 2014*, subsection 16F.

52 Purpose 1 is to 'Protect Australia from national security and criminal threats through effective national coordination, policy and strategy development, emergency management, and regional cooperation.' The other two purposes relate to a: prosperous and united society; and Border and customs operations.



53 Department of Home Affairs, *Corporate Plan 2020–21*, 2020, p.22.

54 Department of Finance, *Developing good performance information — Resource Management Guide No.131*, DoF, 2020, available from <https://www.finance.gov.au/government/managing-commonwealth-resources/developing-good-performance-information-rmg-131> [accessed on 21 December 2021].

- (d) where reasonably practicable, comprise a mix of qualitative and quantitative measures;
- (e) include measures of the entity's outputs, efficiency and effectiveness if those things are appropriate measures of the entity's performance; and
- (f) provide a basis for an assessment of the entity's performance over time.⁵⁵

2.43 Table 2.2 below, details the ANAO's assessment of the department's performance measure.

Table 2.2: Assessment of the department's external critical infrastructure related performance statement measure

Performance measure	Related ^a	Measurable ^b
Effective policy development, coordination and industry regulation safeguards Australia's critical infrastructure against sabotage, espionage and coercion.		

Key:  = Fully meets the requirements of section 16EA of the PGPA Rule.

 = Does not meet the requirements of section 16EA of the PGPA Rule.

Note a: Related refers to the requirement of subsection 16EA(a) of the PGPA Rule, as amended. In applying the related criterion, the ANAO assessed whether the entity's performance measure relate directly to one or more of the entity's purposes or key activities.

Note b: In applying the 'measurable' criterion, the ANAO assessed whether the entity's performance measure was:

- reliable and verifiable — use sources of information and methodologies that are reliable and verifiable; and
- free from bias — provide an unbiased basis for the measurement and assessment of the entity's performance.

Source: ANAO analysis based on Department of Finance's Resource Management Guide No.131.

2.44 The department's critical infrastructure related performance measure is not adequate. The measure:

- relates directly to the department's purposes⁵⁶;
- is not measurable on the basis that targets are not supported by a verifiable method⁵⁷ (see Table 2.3), are not free from bias, and do not include details about how performance against them contribute to achieving the purpose⁵⁸; and

55 The ANAO did not consider the requirements of the PGPA Rule subsections 16EA(d) or 16EA(e) as the audit is only concerned with measure 1.1.3 related to critical infrastructure, not whole Outcome or the entire suite of measures.

56 Portfolio Budget Statement Program 1.7: National Security and Criminal Justice. This program contributes to building a safe and secure Australia by providing comprehensive policy and planning development, at strategic and operational levels, on national security, elements of criminal justice and law enforcement related functions.

Portfolio Budget Statement Purpose 1: Protect Australia from national security and criminal threats through effective national coordination, policy and strategy development, emergency management, and enhanced response, recovery and resilience arrangements.

Corporate Plan Purpose 1: Protect Australia from national security and criminal threats through effective national coordination, policy and strategy development, emergency management, and enhanced response, recovery and resilience arrangements.

As per subsection 16EA(a) of the PGPA Rule and in relation to Portfolio Budget Statement Objective 1.1: Effective policy development, coordination and industry regulation safeguards Australia's critical infrastructure against sabotage, espionage and coercion.

57 *Public Governance, Performance and Accountability Rule 2014*, subsection 16EA(b).

58 *Public Governance, Performance and Accountability Rule 2014*, subsection 16EA(c).

- has targets that relate to outputs.⁵⁹

Table 2.3: Department and ANAO performance target assessments

Target and entity assessment	Methodology	ANAO summary assessment
1.1.3.1: Engage with 100 per cent of entities on the <i>Security of Critical Infrastructure Act 2018</i> register in relation to security and resilience. This metric was assessed as met by the department in 2020–21.	Assessment of the proportion of entities on the SoCI Act register that the Department provides security and resilience advice through ongoing compliance activities, bilateral engagements and participation in relevant industry fora. 'Engagement' is defined as any form of communication with registered entities. For example phone, email, face-to-face meeting.	An internal review noted that 42 per cent of the progress against this metric was due to an advisory email sent to entities being considered as engagement. Likewise, in 2020–21, contact with entities to request they notify the department of any changes was treated as engagement against this target.
1.1.3.2: 100 per cent of notifications received under the Telecommunications Sector Security (TSS) reforms to the <i>Telecommunications Act 1997</i> are responded to within statutory timeframes This metric was assessed as met by the department in 2020–21.	Assessment of the number and percentage of notifications responded to within statutory timeframes of 30 calendar days for notifications and 60 calendar days for notification exemption requests.	The methodology does not specify: <ul style="list-style-type: none"> • the location of the data that supports the method; • repeatable target performance calculations; or • where results are recorded.
1.1.3.3: 100 per cent of Foreign Investment Review Board cases referred are responded to within agreed timeframes. This metric was assessed as partially met by the department in 2020–21.	Assessment of cases referred to the Department that are responded to within timeframes agreed with Treasury.	In 2020–21, performance against the department's target of 100 per cent of Foreign Investment Review Board cases referred to it being responded to within agreed timeframes included counting the 60 per cent of responses when an extension to the original agreed standard response timeframe was sought by the department.
1.1.3.4: Deliver an enhanced framework to protect critical infrastructure and systems of national significance. This metric was assessed as partially met by the department in 2020–21.	Demonstrated progress in delivering legislative amendments, a new Critical Infrastructure Resilience Strategy and an enhanced Trusted Information Sharing Network.	At the time of 2020–21 reporting against the target a new strategy and enhanced network had not been delivered, and legislative amendments had not been enacted.

Source: ANAO analysis based on Department of Finance's Resource Management Guide No.131.

⁵⁹ *Public Governance, Performance and Accountability Rule 2014*, subsection 16EA(e).

Regulatory performance framework self-assessment

2.45 The Regulator Performance Framework, released in October 2014, requires Australian Government regulators to publish annual self-assessments of their performance against six performance indicators. The Regulator Performance Framework notes that ‘for a small number of regulators, issues concerning national security and operational details to achieve regulatory objectives may require published report(s) to be less detailed.’ The department advised the ANAO that it had interpreted this as meaning that the appropriate minister could decide to exempt certain regulatory functions from reporting on national security grounds.

2.46 A ministerial decision approved reporting content, and noted that some functions were excluded on national security grounds, though it did not list critical infrastructure functions as exempt. Rather, the Minister for Home Affairs was advised by the department that ‘exemptions on national security grounds would cover a range of departmental functions’. Although the exemption was only for public reporting of assessments against the framework, the department did not complete any self-assessment of its critical infrastructure related regulatory responsibilities for internal use.

2.47 In July 2021, the Regulator Performance Guide superseded the 2014 Framework. In October 2021, the department advised the ANAO that ‘from 2020–21 it will report directly against the Regulator Performance Framework’. The 2020–21⁶⁰ report for the department did not refer to critical infrastructure related regulatory functions. Annual reporting on the use of powers under the SoCI Act and TSSR does not include performance measurement information.

Legislative reform

2.48 Reform of critical infrastructure related legislation has provided the department with an opportunity to review its performance internally and through external processes. These reforms have allowed the department to review its performance by drawing on external feedback sources in the form of parliamentary activity and stakeholder consultations. Reforms to the SoCI Act in 2021 were developed after consultation processes that are summarised in Appendix 3. The department used content from submissions by its stakeholders to the Parliamentary Joint Committee on Intelligence and Security (PJCIS)⁶¹, and its own consultations to analyse the policy issues associated with the proposed legislative reforms. Submissions to the PJCIS by the department referred to a number of changes made to the Bill following receipt of stakeholder feedback ‘to ensure that the Bill appropriately meets the needs of both Government and owners and operators of critical infrastructure’.⁶²

2.49 In its advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and statutory review of the SoCI Act 2018, the PJCIS recognised these processes and their intent, as well as negative feedback on the lack of action or acknowledgement of input submitted as part of consultations, or sufficient promotion of the opportunity to engage the department on

60 Department of Home Affairs, *Regulator Performance Framework self-assessment report 2020–21* [Internet], DHA, 2021, available from <https://www.homeaffairs.gov.au/access-and-accountability/our-commitments/campaign-and-reform/regulatory-reform> [accessed on 4 January 2022].

61 This includes PJCIS reviews of both the SoCI Act and TSSR.

62 Department of Home Affairs, *Department of Home Affairs submission into the Review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*, DHA, 2021, pp.19–20.

the reforms.⁶³ Notwithstanding a diversity of views on whether engagement provided genuine opportunity to influence legislative reforms, the department provided policy advice to the government on regulatory changes after undertaking consultative processes.

Internal performance information

2.50 Internal monitoring of performance using well-defined measures can be a valuable source of information for a regulator on the effectiveness of its strategies and areas for improvement. The department has established reporting to internal governance bodies on the performance against its business plan and the implementation of government objectives. Measures are well defined and provide updates on the extent to which activities have been implemented or further action is required.

2.51 Performance measures are also included in the Critical Infrastructure Resilience Strategy plan. An internal assessment of progress against activities in the Critical Infrastructure Resilience Strategy did not provide assurance of the progress made, had few references to outputs delivered by activities, and did not assess progress against outcomes.

Recommendation no. 3

2.52 The Department of Home Affairs ensure performance measurement:

- (a) in its corporate plan is adequate and measurable;
- (b) aligns with the Regulator Performance Guide; and
- (c) is used to inform policy and regulatory improvements.

Department of Home Affairs response: *Agreed.*

2.53 *The department agrees to recommendation 3 of the report and acknowledges the areas for improvement identified within its 2020–21 Performance Framework, specifically as they relate to Critical Infrastructure activities. As an immediate initiative, CISC has amended its critical infrastructure performance metrics for 2022–23 to align with the improvements identified by the ANAO. The department continues to mature its framework and performance reporting process to align to best practice principles and welcomes the commentary that its internal measures are well defined and provide updates on the extent to which activities have been implemented. The department notes that recommendation (3b), regarding alignment to the May 2021 Regulator Performance Guide, did not apply to the financial years assessed as part of the Audit. In addition, the Department notes it is not required to measure regulator performance through the Corporate Plan and Annual Report (under the Public Governance Performance and Accountability Act 2013 (PGPA Act) until the 2022–23 financial year.*

63 Parliament of Australia, *Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018*, PJCIS, 2021, p.19.

3. Compliance activities

Areas examined

This chapter examines whether the Department of Home Affairs effectively administered its compliance activities consistent with critical infrastructure protection requirements.

Conclusion

The department's administration of compliance activities consistent with critical infrastructure protection requirements is partly effective. The department's compliance framework does not reflect existing responsibilities or compliance requirements. Compliance activities are not supported by approved procedures or systems controls. The department has not established a risk-based decision framework for achieving compliance outcomes or demonstrating its impact on asset security or resilience. The department does not have a process of effectively reviewing its use of regulatory tools, impact on industry or to inform continuous improvement.

Areas for improvement

The ANAO made four recommendations aimed at improving the department's existing framework to manage compliance, support and review the effective use of all available regulatory tools.

3.1 Effective critical infrastructure regulation is important because a disruption 'could have serious implications for business, governments and the community, impacting supply security and service continuity'.⁶⁴ To assess whether the Department of Home Affairs (the department) effectively administered compliance activities consistent with critical infrastructure protection requirements, the ANAO examined: the department's compliance framework; compliance procedures; and compliance activities.

Has an effective framework been established to manage compliance with critical infrastructure requirements?

The department has established a compliance framework comprised of the Critical Infrastructure Resilience Strategy, Compliance Strategy and Administrative Guidelines. This framework would be enhanced by updating documents in the framework to align with, and clarify, the department's existing responsibilities and regulatory posture.

3.2 A compliance framework is a set of plans, policies, or procedures that set the approach taken to manage compliance. Establishing and implementing appropriate plans supports regulators to achieve desired regulatory outcomes. The framework for the department's compliance approach is summarised in Table 3.1.

64 Department of Home Affairs, *Security Coordination Critical Infrastructure Resilience* [Internet], DHA, 2020, available from <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience> [Accessed on 15 March 2022].

Table 3.1: Summary of critical infrastructure compliance framework

Document	Summary of compliance issues covered
Critical Infrastructure Resilience Strategy	Includes a plan and a policy statement. The policy statement states the 'Australian Government takes a non-regulatory approach to critical infrastructure resilience, favouring a productive business-government partnership' ^a
Critical Infrastructure Centre Compliance Strategy	Outlines the department's approach to compliance under both the <i>Security of Critical Infrastructure Act 2018</i> (SoCI Act) and Telecommunications Sector Security Reforms (TSSR). It states that the Centre's 'vision for Australia's critical infrastructure is one of voluntary compliance by owners and operators, with the Centre as an industry resource, whereby industry and government work cooperatively to jointly manage security risks.' ^b
TSSR Administrative Guidelines	Designed to help entities covered under the TSSR to understand and comply with requirements. The Administrative Guidelines state that 'enforcement mechanisms are intended as a last resort to address non-cooperative conduct rather than to penalise action and decisions taken in good faith' ^c

Note a: Australian Government, *Critical Infrastructure Resilience Strategy: Policy Statement* [Internet], Department of Home Affairs, 2015, available from https://www.cisc.gov.au/help-and-support-subsite/Files/critical_infrastructure_resilience_strategy_policy_statement.pdf [accessed 5 January 2022].

Note b: Australian Government, *Critical Infrastructure Resilience Strategy: Plan* [Internet], Department of Home Affairs, 2015, available from https://www.cisc.gov.au/help-and-support-subsite/Files/critical_infrastructure_resilience_strategy_plan.pdf [accessed 5 January 2022].

Note c: Department of Home Affairs, *Telecommunications Sector Security Reforms (TSSR) Administrative Guidelines* [Internet], Department of Home Affairs, 2015, available from www.cisc.gov.au/help-and-support-subsite/Files/tss_administrative_guidelines.pdf [accessed on 5 January 2022].

Source: ANAO analysis of departmental documentation.

3.3 The department's compliance framework outlined in Table 3.1 does not reflect its current compliance requirements. The Critical Infrastructure Resilience Strategy, which guides the work of the Cyber and Infrastructure Security Centre, has not been updated since 2015, despite including a review point in 2020, and plans by the department to update it since at least 2019. Consequently, the Critical Infrastructure Resilience Strategy does not:

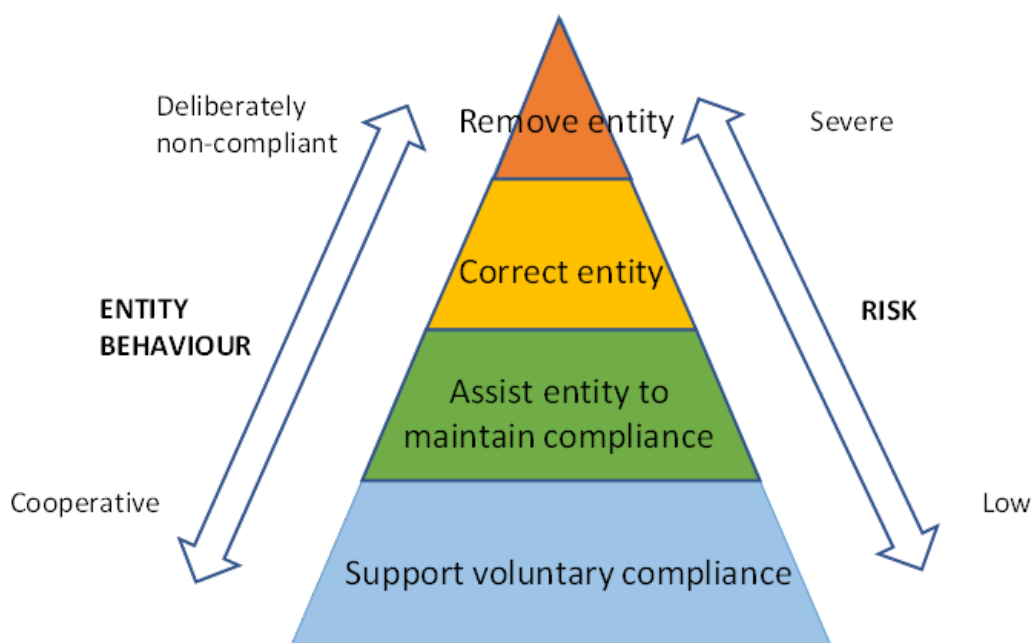
- reflect machinery of government changes in 2017 that moved responsibility for critical infrastructure protection coordination to the department;
- delineate the department's policy and regulatory responsibilities from those of other Commonwealth, state and territory regulatory bodies, or set out how these responsibilities will be applied; or
- align with current powers to regulate critical infrastructure, or the increased scale and sophistication of threats that have been used as the basis for legislative changes but not reflected in the compliance framework.

3.4 Figure 3.1 illustrates the compliance model included in the compliance strategy, with the following tools listed under each of the four tiers in the model.

- Support voluntary compliance: information exchange, guidance and advice, validation of compliance activities.
- Assist entity to maintain compliance: education and training, threat advice, sharing best practice information, set clear expectations and standards.
- Correct entity: formal warnings, ministerial directions, injunctions, enforceable undertakings, civil penalties, prosecution.

- Remove entity: cancel licence to operate, divestment order, regulator step-in, ministerial directions.

Figure 3.1: Critical Infrastructure Centre compliance model



Source: Department of Home Affairs, *Critical Infrastructure Centre Compliance Strategy*, DHA, 2019, p.6, available from: <https://www.cisc.gov.au/help-and-support-subsite/Files/critical-infrastructure-centre-compliance-strategy.pdf> [accessed on 5 January 2022].

3.5 The compliance framework includes actionable activities that are tracked over time and publicly reported. The Critical Infrastructure Centre Compliance Strategy states that the department ‘will conduct monitoring activities to assess entity compliance with their obligations under the [SoCI] Act, the TSSR and to support Treasury’s compliance activities under the [*Foreign Investment and Takeovers Act 1975* (FATA)]’.

3.6 The strategy states that monitoring activities for the three Acts may include: entity reporting requirements, information gathering, inspection and retention of documents, audits by the Centre or authorised representatives and assessing compliance.

3.7 Compliance framework documents do not specify the circumstances that would trigger or inform decisions to undertake compliance activities. There is also no reference to situations where the powers of other stakeholders would be supported or used instead of those of the department or the Minister for Home Affairs (such as in section 32 or section 51 of the SoCI Act).⁶⁵

⁶⁵ See ministerial direction powers in Table 3.2.

Recommendation no. 4

3.8 The Department of Home Affairs revise or replace the Critical Infrastructure Resilience Strategy with documentation that reflects current policy, regulatory responsibilities and posture, and outlines its application by the department in relation to other critical infrastructure asset sector policy leads and regulators.

Department of Home Affairs response: *Agreed.*

3.9 *The department agrees to recommendation 4 of the report. The Critical Infrastructure Resilience Strategy is under revision for release in 2022 following passage of the critical infrastructure security reforms. The department is currently engaging with government and industry on a refreshed Critical Infrastructure Resilience Strategy which reflects the significant policy advance following amendments of the Security of Critical Infrastructure Act 2018 (SoCI Act) in December 2021 and March 2022. The refreshed Critical Infrastructure Resilience Strategy clearly articulates the roles and responsibilities of Commonwealth and State and Territory governments and critical infrastructure entities in ensuring the continued delivery of the essential services all Australians rely upon.*

Are effective procedures and systems in place to support the use of regulatory tools?

The majority of policy and procedural documents (15 of 22) to support possible critical infrastructure-related compliance activities were drafted, but not finalised and approved, or included in the department's policy and procedural repository. A lack of procedures, or procedures that remain in draft, increases the risk of inconsistency in administration and decision-making. The department does not have an established process to ensure that appropriately trained officials are engaged in investigations under critical infrastructure regulations. Classified network and critical infrastructure-related system security controls do not meet the requirements to mitigate the risk of unauthorised access.

3.10 Australian Government policy requires regulators 'to weigh the efficiency and cost-effectiveness of their regulatory actions, seeking to impose the least burden on those that are regulated while maintaining essential safeguards'.⁶⁶

Procedures

3.11 Establishing appropriate procedures and systems helps ensure regulatory tools can be used as intended, achieve desired outcomes, and are used in a legally sound and defensible manner. This includes implementing policies, procedures and supporting documentation, establishing appropriate information systems, ensuring staff are appropriately trained and qualified, and ensuring regulatory powers have been legally delegated to officials.

3.12 The department has:

⁶⁶ Department of the Prime Minister and Cabinet, *Regulator Performance Guide*, PM&C, 2021, p.8.

- thirteen draft procedures relating to regulatory powers under the SoCI Act. None have been finalised, approved or included on the department's policy and procedural repository; and
- nine policies and procedures that relate to regulatory powers under the TSSR, two of which have not been finalised, approved and included on the department's policy and procedural repository.

3.13 Most of the unapproved SoCI Act procedures were drafted in 2019 and 2020. The ANAO was advised that procedures are in use despite not being finalised and some having drafting comments in them.

3.14 The department's Critical Infrastructure Compliance Strategy identifies its 'correct' compliance model tier as applying injunction, civil penalty, and enforceable undertaking powers in instances where:

engagement, negotiation, or mediation are unsuccessful, or where the Centre believes the entity is not acting in good faith, the Centre will escalate to enforcement measures to achieve compliance and mitigate the identified risk.⁶⁷

3.15 Application of these enforcement measures may involve conducting investigations as a process of seeking information relevant to an alleged, apparent or potential breach of the law, involving possible judicial proceedings.⁶⁸ The department does not have established procedures to manage circumstances where an investigation may be required. This procedure should specify how investigations will be conducted and identify minimum training or qualifications standards required by Australian Government agencies for investigations staff.⁶⁹

3.16 The department's delegation of powers to apply the enforcement measures was consistent with legislative requirements.

Information systems

3.17 The department uses a secure information technology platform to store classified material that relates to critical infrastructure assets. Procedures exist that outline how information is transferred from a webform portal to the secure platform. Controls and classification during this transfer were applied appropriately.

3.18 A core group of personnel are relied on to administer, update and use the secure database in response to more diverse and increasing requests for asset information. There would be merit in the department establishing records, controls, or contingency plans to manage, or respond to advice requests based on critical infrastructure data in circumstances where this core group of personnel are unavailable.

67 Department of Home Affairs, *Critical Infrastructure Centre Compliance Strategy*, DHA, pp.7–8.

68 Australian Government, *Australian Government Investigations Standards* [Internet], Attorney-General's Department, 2011, available from <https://www.ag.gov.au/sites/default/files/2020-03/AGIS%202011.pdf> [accessed 5 January 2022], p.1. The Australian Government Investigations Standards states that 'the primary purpose of an investigation is to gather admissible evidence for any subsequent action, whether under criminal, civil penalty, civil, disciplinary or administrative sanctions'.

69 *ibid.* The Australian Government Investigations Standards are mandatory for all agencies required to comply with the *Public Governance, Performance and Accountability Act 2013*.

3.19 The department has appropriate information technology systems controls to ensure that critical infrastructure administration is conducted in accordance with protective security requirements. The systems and their controls rely on manual processes to remove users when they no longer occupy roles that require access to secure systems, or undertake analysis that underpins critical infrastructure advice.

3.20 A classified system is used to store critical infrastructure related information. While the department has technical security design, procedures and risk assessment documents relating to the network and systems, two security controls established for the classified network and critical infrastructure systems were not implemented in accordance with Protective Security Policy Framework and Information Security Manual requirements. This increases the risk of unauthorised access to classified systems and information.

Recommendation no. 5

3.21 The Department of Home Affairs support effective use of the full suite of available critical infrastructure related regulatory tools by having in place procedures that:

- (a) are finalised, approved and lodged on the internal policy and procedural repository;
- (b) ensure trained officials are appropriately engaged in investigations; and
- (c) align with the Protective Security Policy Framework and Information Security Manual requirements.

Department of Home Affairs response: *Agreed.*

3.22 *The department agrees to recommendation 5 of the report. The department notes the audit report finding that the critical infrastructure compliance framework should be updated to reflect current responsibilities. The CISC was established on 1 September 2021 to bring together the critical infrastructure regulatory functions of the department. The Centre released in April 2022 its new Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy that guides effective use of its regulatory tools. The CISC has developed an updated risk-based compliance regulatory framework, with a particular focus on its new regulatory powers arising from amendments to the SOCI Act. As part of this the CISC is also reviewing and updating critical infrastructure compliance policies and procedures in light of the amendments to the SOCI Act.*

Is the use of regulatory tools consistent with legislative and procedural requirements?

The department's use of regulatory tools is not always consistent with legislative and procedural requirements, and approved procedures or decision records do not exist for all compliance activities and outcomes. Use of regulatory tools was consistent with the department's documented regulatory posture. Decisions on whether to escalate to higher tiers of the regulatory compliance model were not supported by approved procedures, processes, or documented analysis of the administrative or financial burden associated with an escalation of compliance activity.









3.23 Australian Government regulators draw authority from, and are subject to, a range of legal and other requirements. Effectively implementing a compliance program requires that a regulator

act on identified instances of non-compliance. If actions are not escalated in accordance with regulatory powers, the impact of the regulator and the achievement of regulatory outcomes may be diminished.


3.24 The department's critical infrastructure related regulatory functions and powers under the SoCI Act and TSSR are summarised in Table 3.2.

Table 3.2: Summary of regulatory functions and powers under critical infrastructure-related legislation

Function or power	SoCI Act ^a	TSSR
Register of Critical Infrastructure Assets	✓ Section 19	✗
Notification requirement	✓ The responsible entity for a critical infrastructure asset has initial and ongoing reporting obligations. It may be required to report a cyber security incident. Sections 23, 24, 30BC and 30BD	✓ Carriers and nominated carriage service providers must notify intention to implement a proposed change if the change is likely to have a material adverse effect on their capacity to comply with security obligations. An exemption to notify proposed changes can be granted. The carrier or provider may be required to provide further information. A Security Capability Plan covering 12 months can be provided to notify one or more proposed changes. Sections 314A, 314B(1) and 314C
Written notice of assessment	✗	✓ If a risk is found, the Communications Access Coordinator ^a (CAC) will advise the carrier or provider. The CAC may set out measures the carrier or provider could adopt to eliminate or reduce the risk. Subsections 314B(3) and 314B(4)
Ministerial direction	✓ Minister may direct an owner or operator of critical infrastructure assets to mitigate national security risks under certain conditions. Minister may privately declare ^b an asset to be critical infrastructure. In response to a cyber security incident, the Secretary may require an entity or request an authority agency to undertake actions. Sections 32, 35AQ, 35AX and 51	✓ Minister may direct carrier or carriage service provider to undertake actions if certain criteria are met. Sections 315A and 315B

Function or power	SoCI Act ^a	TSSR
Information gathering	 Secretary may require an entity to provide certain information and documents. The Secretary may direct an entity to provide information in relation to a cyber security incident. Sections 35AK and 37	 Secretary can require certain information and documents that are relevant to assessing compliance. Section 315C
Injunction	 Section 49	 Section 564
Civil penalty	 Section 49	 Section 570
Enforceable undertaking	 Section 49	 Section 572

Key:  = power is legislated.

 = power not legislated.

Note a: The Communications Access Coordinator (CAC) is the Secretary of the department or a person, or body specified by the Minister as set out in section 6R of the *Telecommunications (Interception and Access) Act 1979*. The CAC liaises between security and law enforcement agencies and the telecommunications industry.


Note b: The Minister for Home Affairs added privately declared assets to the register using a direction power under the SoCI Act. This power was used in 2018.

Source: ANAO analysis.






3.25 The powers under the TSSR with approved and finalised procedures had been consistently applied.⁷⁰


3.26 The Critical Infrastructure Centre Compliance Strategy lists tools that will be used against the four tiers of non-compliance ranging from support, assist, correct, to remove. The strategy describes seeking compliance outcomes through a non-regulatory approach for entities covered under both Acts. Table 3.3 shows the use of critical infrastructure related regulatory tools available under both Acts against each tier of the compliance model.




Table 3.3: Use of regulatory tools to respond to potential non-compliance

Tier	Tools	ANAO assessment of the use of tools by the department	
Support voluntary compliance	Information exchange		The department reported that in 2020–21: <ul style="list-style-type: none"> the Communications Access Coordinator received 30 notifications about proposed changes (subsection 314A(3) of the <i>Telecommunications Act 1997</i>); and there were 223 notifications made to the department. This included 11 new notifications and 212 notifications of changes (sections 23 and 24 of the SoCI Act).

⁷⁰ See paragraphs 3.12 and 3.13 for those procedures that were not finalised and approved.

Tier	Tools	ANAO assessment of the use of tools by the department	
	Guidance and advice		<p>The department reported that in 2020–21, it:</p> <ul style="list-style-type: none"> participated in 98 engagements to ensure telecommunications industry participants understood their security and notification obligations and to provide advice on proposed changes to telecommunications systems and services; held technical workshops with specific carriers to explore changes; and engaged with critical infrastructure stakeholders through 'meetings, telephone, email, and formal website enquiries'.^a <p>The department has webpages covering requirements under both Acts.</p>
	Validation of compliance activities		<p>The department has undertaken some validation of compliance activities under both Acts.</p> <ul style="list-style-type: none"> TSSR — to ensure that high priority entities engaged with the department about their obligations. When entities did not engage, the department did not have a recorded decision to cease or not escalate compliance activity. SoCI Act — to ensure that entity information was registered with the department. Records do not confirm compliance for all registered assets. <p>The department has worked with other regulators to conduct audit activities as listed in the strategy.</p>
	Education and training		<p>The department provides informal education and training in the form of updates to industry and other regulators through stakeholder engagement and information on its website. Formal education and training has not been provided to relevant stakeholders under both Acts.</p>
Assist entity to maintain compliance	Threat advice		<p>Threat advice was issued via the department website and engagement forums.</p>
	Sharing best practice information	Not used	
	Set clear expectations and standards		<p>Correspondence with entities, the TSSR Administrative Guidelines, and notices issued to carriers from the Communications Access Coordinator under TSSR were used to encourage compliance under the Telecommunications Act. Correspondence with entities was used to encourage compliance under the SoCI Act.</p>

Tier	Tools	ANAO assessment of the use of tools by the department	
	Formal warning		In 2019, letters were sent to selected entities that had not engaged with the department on their TSSR obligations. The department's records do not identify why compliance was not escalated for an entity that was unresponsive as at the end of 2021. Since November 2018, further information was sought for 36 per cent of TSSR notification cases. Despite these requests including a warning that not responding may result in the use of information gathering powers, the powers were not used.
Correct entity	Ministerial direction ^a	Not used.	
	Injunctions Enforceable undertaking Civil penalties Prosecution	Not used.	
Remove entity	Cancel licence Divestment order Regulator step-in Ministerial direction ^b	Not used.	

Key:  = Tool used to manage compliance.
 = Tool used in some compliance activity.
 = Tool used and potential non-compliance not managed.

Note a: This includes the activity measured under performance statement target 1.1.3.1 listed in Table 2.3.

Note b: In 2018, the Minister for Home Affairs added privately declared assets to the register using a direction power under the SoCI Act. This is not the direction power referred to under the compliance model.

Source: ANAO analysis of departmental documentation.

3.27 Consistent with the department's regulatory posture, the focus of regulatory activity has been to support voluntary compliance and assist entities to maintain compliance. This approach was identified in the annual reporting of powers under the TSSR and SoCI Act to:

- achieve 'national security outcomes on a cooperative basis rather than through the formal exercise of regulatory powers'⁷¹; and
- enable government 'to better assess the extent of vulnerability across our high priority assets ... while maintaining open economic settings and imposing only a minimal and targeted regulatory burden'.⁷²

3.28 In its submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) statutory review of Part 14 of the Telecommunications Act, the department noted that while its:

primary focus is to achieve national security outcomes on a cooperative basis, the Act allows the Minister for Home Affairs to seek an injunction requiring a notification, accept an enforceable undertaking or pursue civil penalties in relation to non-compliance with s314A(3) of the Act.

71 Department of Home Affairs, *Telecommunications Sector Security Reforms, 2020-21 Annual Report* [Internet], DHA, 2021, available from <https://www.homeaffairs.gov.au/nat-security/files/telecommunications-sector-security-reforms.pdf> [accessed 5 January 2022].

72 Department of Home Affairs, *Security of Critical Infrastructure Act 2018, 2020-21 Annual Report* [Internet], DHA, 2020, available from <https://www.homeaffairs.gov.au/nat-security/files/security-of-critical-infrastructure.pdf> [accessed 5 January 2022].

However, there is significant administrative and financial burden associated with these enforcement measures and may not be the most appropriate mechanism to achieve an appropriate security outcome.

3.29 While the statements in the department's submission are also consistent with its compliance posture, it has not measured the administrative or financial burden of using tools available in the higher tiers of its compliance model.

Is there an effective process to identify non-compliance?

The department does not have an established process to obtain assurance of regulatory compliance. This limited the department's capacity to demonstrate that it has a proportionate and effective approach to resolving non-compliance, or has improved the security or resilience of critical infrastructure assets.

3.30 Risk-based regulation is important in ensuring that the burden of regulation is appropriate. It is successful when available evidence is used to develop a strategic, diligent and risk-based regulatory compliance approach, and this approach is consistently implemented. Too strong a focus on 'red tape' reduction, including through not utilising the full range of regulatory powers provided by the Parliament, can be at the expense of effective outcomes.

Risk-based compliance

3.31 The department's enterprise risk management framework aims to fully integrate risk management in planning and decision-making activities. The Regulator Performance Guide, sets out the benefits of regulators properly assessing and responding proportionately to risks of non-compliance, stating that:

[s]trategic management of risk can also improve efficiency by prioritising resources to the areas of highest risk, and increase compliance by focusing limited resources on the areas of the greatest risk of non-compliance. It can also reduce the overall compliance and cost burden by minimising Government intervention where the risks are relatively low.⁷³

3.32 Table 3.3 shows that the department adopted a risk-based approach to prioritise its compliance activities and use of resources. Support for voluntary compliance activities included a high proportion of entities covered under the TSSR and SoCI Act, and high priority entities were identified and engaged in follow-up activities to validate compliance or encourage further information to be submitted to ensure compliance. The process for identifying high priority entities was limited by the absence of a defined non-compliance risk assessment process, and adjustments to this process based on factors such as compliance activity outcomes or the threat environment in which the activity is being undertaken.

Compliance actions

3.33 The Critical Infrastructure Centre Compliance Strategy states that the Centre 'will facilitate full compliance by critical infrastructure owners and operators with their obligations under legislation and, where applicable, FATA conditions'. The Centre's website also states that it 'works closely with industry, states and territories, regulators and technical advisers'.

⁷³ Department of the Prime Minister and Cabinet, *Regulator Performance Guide*, PM&C, 2021, p.9.

3.34 The department has not measured whether full compliance has been achieved because it has not confirmed all entities covered by the SoCI Act and the TSSR are compliant. The department's records did not identify when decisions were made to:

- not engage with some entities about their compliance with relevant legislation until two years after it had commenced (see Case study 1); or
- not finalise compliance activities that commenced in 2019 for all SoCI Act assets (see Case study 2).

Case study 1.

In 2019, the department wrote to 10 select telecommunications carriers that had not engaged with the department about their TSSR obligations. In June 2020, the department noted that one of the carriers had still not engaged with the department. While the department made several attempts to contact the carrier's new owners, as at November 2021 it had not received a response. The department has not identified why compliance actions were not escalated.^a

In June 2020, the department identified priority carriers and carriage service providers that had little or no engagement with the department about their TSSR obligations. The department requested meetings with most of these entities to discuss their obligations. The department did not successfully arrange meetings with all entities. The department also did not document why non-responses by some entities to meeting requests were not followed up.

The meetings that were arranged occurred in mid-late 2020. According to meeting minutes, some entities were not aware of any or all their TSSR obligations. It had been approximately two years since the TSSR commenced (18 September 2018).

Note a: The department advised the ANAO that 'due to resourcing constraints and other high priority tasks at the time, compliance actions were not escalated'.

Case study 2.

Under the SoCI Act, the responsible entity for a critical infrastructure asset must submit operational information in relation to the asset. Following a six month grace period for information to be submitted voluntarily, the department commenced an initial analysis of information submitted by the entity to the register to inform its compliance approach. Compliance activities commenced in April 2019, and an initial assessment resulted in all assets being categorised against five compliance categories. Department records identify that compliance activities for only one category were finalised. The process was not completed for all assets.

3.35 The department does not have an established system to monitor existing critical infrastructure related compliance activity to inform decisions to consistently trigger, triage and manage cases. An established system should document decisions made to:

- use a power, or to not use it where a circumstance arises where it could be used;
- escalate, or not escalate a case to a higher compliance model tier; or
- not pursue further activity, or close a case.

3.36 Between October 2018 and September 2021, the department recorded receipt of 161 TSSR notifications lodged by entities covered under the TSSR. Of these 161 notifications, 57 (35 per cent)

were assessed as requiring further information about the proposed change before a security assessment could be completed. A review of 12 (21 per cent) notification cases where further information was sought found that the department's handling under the TSSR was consistent with legislative and procedural requirements.

- None of the cases sampled, that were subject to requests for further information from an entity, resulted in a final assessment of residual concerns being made by the appropriate delegate in the department that documented the decision to use or not use further regulatory tools available to them, or that concerns had been addressed.
- All requests had a 30-day timeframe for the information to be provided, and a warning that the information gathering power may be used if there was no response. For one example, where a change submitted under the TSSR had raised national security concerns, the department had not concluded its compliance activity or used its regulatory tools in the higher tiers of its compliance model 18 months after the change was submitted.

3.37 In its submission to the PJCIS statutory review of Part 14 of the Telecommunications Act, the department noted challenges in ensuring changes made by carriers were appropriately notified or that risks were mitigated.⁷⁴ The department's submission did not substantiate why the information gathering power under the TSSR is not used in those instances where further information was required to complete notification assessments. A procedure to use the information gathering power was drafted but not finalised or approved.

3.38 While draft procedures exist on regulatory powers at higher tiers of the department's compliance model, they did not set out circumstances when no further action was necessary or when it would be appropriate to escalate matters from business-as-usual monitoring to compliance activity, or to higher tiers. A documented triage process would support the department to document compliance outcomes and escalate the most important matters for further action and resolution. The *Australian Government Investigation Standards* states that agencies should have written procedures that outline how the initial evaluation and actioning of matters will occur.⁷⁵

74 Department of Home Affairs, *Parliamentary Joint Committee on Intelligence and Security statutory review of Part 14 of the Telecommunications Act 1997 Submission No.34*, DHA, November 2020.

75 See sections 2.2 and 2.3 of Australian Government, *Australian Government Investigation Standards* [Internet], Attorney-General's Department, 2011, available from <https://www.ag.gov.au/sites/default/files/2020-03/AGIS%202011.pdf> [accessed 5 January 2022].

Recommendation no. 6

3.39 The Department of Home Affairs approve, apply and monitor consistent use of policies, procedures and processes to:

- (a) trigger, triage and manage escalated use of critical infrastructure compliance powers, including by making better use of its information gathering, and investigatory powers where national security concerns have been identified; and
- (b) revise its risk approach and implement processes that enable effective assessment, prioritisation and management of non-compliance risks.

Department of Home Affairs response: *Agreed.*

3.40 *The department agrees to recommendation 6 of the report. The CISC is designing an updated risk-based compliance regulatory framework, with a particular focus on its new regulatory powers arising from amendments to the SOCI Act.*

Measuring the achievement of outcomes

3.41 Clearly defined, measurable and achievable outcomes are critical to the effective delivery of risk-based regulation.⁷⁶ While the department reports on its use of regulatory tools in annual reporting, it does not report on achievement of its policy statements about how it will support other Commonwealth, state, and territory regulators to ensure the security of critical infrastructure. The Critical Infrastructure Resilience Strategy includes outcomes and activities related to the department working with other regulators.⁷⁷ The department has not reported on the achievement of these outcomes and activities.

3.42 The Critical Infrastructure Centre Compliance Strategy also states that ‘information sharing between government and industry, and across industry, has proven to be an effective mechanism to build organisational and sectoral resilience with minimal government intervention’.⁷⁸ The department’s information sharing is limited to its regulatory functions and does not extend to achieving broader strategic policy outcomes. For example, the NSW Independent and Pricing Regulatory Tribunal (IPART) has included in its licencing conditions that information can be shared with the department, and IPART can receive risk advice from the department to support regulatory activities under the operating licence conditions. The department does not have broader strategic

76 NSW Department of Finance, Services and Innovation, *Guidance for regulators to implement outcomes and risk-based regulation* [Internet], NSW DoF, 2016, p.3, available from [http://productivity.nsw.gov.au/sites/default/files/2018-05/Guidance for regulators to implement outcomes and risk-based regulation-October 2016.pdf](http://productivity.nsw.gov.au/sites/default/files/2018-05/Guidance%20for%20regulators%20to%20implement%20outcomes%20and%20risk-based%20regulation-October%202016.pdf) [accessed 5 January 2022].

77 See Australian Government, *Critical Infrastructure Resilience Strategy*, which includes for example, outcome 1 which is ‘a strong and effective business-government partnership’. Supporting activities include 1.3 ‘A flexible participation model for the Strategy that delivers value to participants, including through enhanced information sharing’ and 1.4 ‘Effective linkages and collaboration between critical infrastructure stakeholders’.

78 Australian Government, *Critical Infrastructure Centre Compliance Strategy* [Internet], Department of Home Affairs, p.4, available from <https://www.cisc.gov.au/help-and-support-subsite/Files/critical-infrastructure-centre-compliance-strategy.pdf> [Accessed on 5 January 2022].

information sharing arrangements in place with similar regulatory bodies in other jurisdictions (see Appendix 4, Table A.6).

3.43 Information sharing that is limited to the department's regulatory functions prevents the department from anticipating and adapting to a wide range of information. It also reduces the visibility of threats and incidents. The department has not established a process to formalise information sharing arrangements between the department and its stakeholders to inform critical infrastructure related regulatory activities of either or both parties.

3.44 In December 2021, the department ran an exercise with state and territory representatives to familiarise them with government assistance measures contained in the SoCI Act as it was amended by the Security Legislation Amendment (Critical Infrastructure) Bill 2021. The purpose was also to identify issues to be considered as part of standard operating procedures for government assistance measures. For example, powers to gather information, to direct an entity to do or refrain from an action, or to request an authorised agency to provide support. The department has not used similar exercises to test whether existing policy outcomes have been achieved.

Has the use of regulatory tools been effectively reviewed?

The department has not established a process to effectively review regulatory tool use, impacts on industry, or lessons learned to inform continuous improvement.

3.45 When regulators measure performance, they should incorporate them into an appropriate monitoring, reporting and evaluation framework that provides assurance over its achievement of objectives, as set out in relevant legislation. Compliance information collected by the regulator will also assist in determining performance against expectations and the impact of regulatory activities over time. Effective review of regulations is a critical element in establishing accountability for program performance, ensuring ongoing improvement, and is an appropriate justification for any regulatory changes.

3.46 The department's Critical Infrastructure Centre Compliance Strategy states that the centre will 'continually review its activities based on the results and impact on industry'. The department has not established a process of reviewing its use of regulatory tools under the SoCI Act or TSSR for measuring the impact on industry of its use of regulatory tools. The performance framework components referred to in paragraphs 2.38 to 2.51 presented opportunities for the department to review the effectiveness and lessons learned from its use of regulatory tools.

Recommendation no. 7

3.47 The Department of Home Affairs evaluate, monitor, and report on:

- (a) the extent to which regulatory tools are used to effectively improve security and resilience of critical infrastructure assets to risks; and
- (b) implementation of actionable items in strategies, reviews and lessons learned for which it is responsible and how they contribute to intended outcomes.

Department of Home Affairs response: *Agreed.*

3.48 *The department agrees to recommendation 7 of the report. The department's evaluation, monitoring and reporting of regulation and regulatory tools is being updated to align with the Government's Deregulation Agenda, the latest Regulator Performance Guide and the regulator performance reporting requirements under the PGPA Act and PGPA Rule. Consistent with this, the CISC is designing an updated risk-based compliance regulatory framework, with a particular focus on its new regulatory powers arising from amendments to the SOCI Act. The Centre released in April 2022 its new Cyber and Infrastructure Security Centre Compliance and Enforcement Strategy that guides effective use of its regulatory tools, and has committed to review this strategy periodically to account for new findings from intelligence, risk evaluation and regulatory engagement.*



Grant Hehir
Auditor-General

Canberra ACT
21 June 2022

Appendices

Appendix 1 Entity response



Australian Government
Department of Home Affairs

Mr Grant Hehir
Auditor-General
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Hehir

Thank you for the opportunity to provide comments on the Australian National Audit Office's (ANAO) report on the *Administration of Critical Infrastructure Protection Policy*.

The Department of Home Affairs (the Department) acknowledges the value of the ANAO providing independent analysis of, and insights into, the effectiveness of the Department's administration and regulation of critical infrastructure protection policy. Undertaking an audit immediately prior to the finalisation of a significant legislative change to the *Security of Critical Infrastructure Act 2018* (an Act that is now 236 pages compared to some 60 pages in 2018) will inform successful implementation.

The report makes seven recommendations to the Department aimed at: the use of risk management to inform decision-making; establishing an engagement strategy; having appropriate performance measurement; improving the Department's existing framework to manage compliance; and support and review the effective use of all available regulatory tools. The Department accepts all of these recommendations.

In relation to recommendation 3, the Department acknowledges the areas for improvement identified within its 2020–21 Performance Framework, specifically as they relate to critical infrastructure activities. As an immediate action, the Department has updated its critical infrastructure performance metrics for 2022/23 and will continue to mature its framework and performance reporting process to align with best practice principles.

The establishment of the Cyber and Infrastructure Security Centre (the CISC) on 1 September 2021 brought together the critical infrastructure regulatory and security risk assessment functions of the Department. The CISC has provided a fundamental opportunity to focus on its risk assessment framework to ensure consistency to support regulatory action, coordination and policy advice.

The Department's evaluation, monitoring and reporting of regulation and regulatory tools is being updated to align with the Government's deregulation agenda, the latest Regulator Performance Guide and the regulator performance reporting requirements under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the *Public Governance, Performance and Accountability Rule 2014* (PGPA Rule). Consistent with this, the CISC is updating its risk-based compliance regulatory framework, with a particular focus on its expanded remit and new regulatory powers arising from amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act).

As part of this, the CISC is also reviewing and updating critical infrastructure compliance policies and procedures to align amendments to the SOCI Act and expanded remit. For example, in April 2022, the CISC released its new CISC Compliance and Enforcement Strategy that guides effective use of its regulatory tools, and has committed to review this strategy periodically to account for new findings from intelligence, risk evaluation and regulatory engagement.

The Critical Infrastructure Resilience Strategy is under revision and was not finalised due to the significance of the legislative reforms in the Parliament – the second tranche of which passed the Parliament on 31 March 2022. The Strategy brings together legislative reforms and non-regulatory initiatives to uplift critical infrastructure security and resilience in the face of all hazards. This is underpinned by a partnerships approach realised through the Trusted Information Sharing Network. A new Critical Infrastructure Resilience

6 Chan Street Belconnen ACT 2617
PO Box 25 Belconnen ACT 2616 • Telephone: 02 6264 1111 • www.homeaffairs.gov.au

Strategy will seek to clearly articulate the roles and responsibilities of Commonwealth and State and Territory governments and critical infrastructure entities in ensuring the continued delivery of the essential services all Australian rely upon given the new legislative definitions and obligations now in force.

As noted by the ANAO, the Department produced sector-specific engagement strategies in 2021 focused on the legislative reforms and how best to support sectors through the reforms journey. The Department agrees that there will be an ongoing need to ensure clarity of responsibility and accountability for ensuring steps are taken to maintain security of Australia's critical infrastructure. The Department continues to mature its framework and performance reporting process to align to best practice principles and welcomes the commentary that its internal measures are well defined and provide updates on the extent to which activities have been implemented.

Please find attached a summary response to the report for inclusion in the formal report (Attachment A), as well as a response to the recommendations (Attachment B). Editorial comments are also provided at Attachment C.

The Department would like to thank the ANAO for their collaborative approach throughout the audit process, including ongoing advice provided, as it relates to maturing its performance framework into 2022–23.

Yours sincerely



Ben Wright
Chief Audit Executive

12 May 2022

Appendix 2 Improvements observed by the ANAO

1. The fact that independent external audit exists, and the accompanying potential for scrutiny, improves performance. Program-level improvements usually occur: in anticipation of ANAO audit activity; during an audit engagement as interim findings are made; and/or after the audit has been completed and formal findings are communicated.
2. The Joint Committee of Public Accounts and Audit (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts.
3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:
 - strengthening governance arrangements;
 - initiating reviews or investigations; and
 - introducing or revising policies or guidelines.
4. In this context, the below improvements were observed by the ANAO during the course of the audit. It is not clear if these actions and/or the timing of these actions were already planned before this audit commenced. The ANAO has not sought to obtain reasonable assurance over the source of these improvements or whether they have been appropriately implemented.
5. Performance improvements observed by the ANAO during the course of this audit were:
 - In September 2021, the Critical Infrastructure Centre was re-branded as the Cyber and Infrastructure Security Centre (see paragraph 1.20);
 - In December 2021, amendments to the *Security of Critical Infrastructure Act 2018* (SoCI Act) expanded the asset classes covered from four to 22 across 11 sectors, and in December 2021 the department commenced consultations on further amendments to the SoCI Act. In March 2022, the *Security Legislation Amendment (Critical Infrastructure Protection) Bill Act 2022* was passed by the Parliament (see paragraph 1.20);
 - In November 2021, the department revised quarter four 2020–21 assessments of its enterprise risk, including its critical infrastructure risk (see paragraph 2.8); and
 - In December 2021, the department ran an exercise with state and territory representatives to familiarise them with government assistance measures contained in the SoCI Act (see paragraph 3.44).

Appendix 3 Timeline of critical infrastructure reform events and implications

Table A.1: Key dates and consequences of changes to Australian Government legislation

Date	Event	Event consequences
6 September 2019	Australia's 2020 Cyber Security Strategy 'A call for views' was released by the Australian Government.	The public was invited to comment on the management of cyber risks and cyber defences on private networks. The department received 215 submissions and met with over 1400 individuals.
21 July 2020	Cyber Security Strategy Industry Advisory Panel final report released. ^a	Among the report's 60 recommendations, the Industry Advisory Panel recommended that the Australian Government: <ul style="list-style-type: none"> • review the definition of critical infrastructure; • introduce reasonable, principles-based requirements for owners and operators of critical infrastructure; and • work with industry to agree where it would be necessary for government to provide reasonable assistance during a cyber security emergency.
6 August 2020	Reforms in Australia's Cyber Security Strategy 2020 released by the Australian Government.	The Australian Government's response to the Cyber Security Strategy Industry Advisory Panel report. The strategy refers to the development of 'an enhanced regulatory framework for critical infrastructure and systems of national significance' that will include: <ul style="list-style-type: none"> • enforceable positive security obligations for designated critical infrastructure entities; • enhanced cyber security obligations for those entities most important to the nation; • Australian Government assistance for businesses in response to the most significant cyber attacks to Australian systems; and • voluntary measures to strengthen engagement with businesses in relation to risk, and support an entity's security uplift.^b
12 August 2020	Protecting Critical Infrastructure and Systems of National Significance consultation paper released by the Minister for Home Affairs.	Consultation included eight town halls, 22 sector-specific workshops and bilateral meetings involving over 2000 participants from more than 540 entities. 194 submissions were received, 128 submissions were published on the department's website, and 66 submissions remain confidential.
9 November 2020	Exposure draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill) and associated documents released by the department for public comment.	The department engaged with over 1000 participants on the Exposure Draft in four town halls and bilateral meetings. The department received 129 submissions.

Date	Event	Event consequences
10 December 2020	The Bill was introduced to Parliament.	<p>The Bill proposed:</p> <ul style="list-style-type: none"> • a Positive Security Obligation for specified critical infrastructure entities. This includes mandatory cyber incident reporting, an expanded application of the existing Register of Critical Infrastructure Assets from four to 11, to require the provision of ownership and operational information, and a risk management program, with this element of the obligation to be co-designed with industry; • enhanced Cyber Security Obligations for those entities most important to the nation (deemed 'systems of national significance'); and • government assistance to protect critical infrastructure assets from serious cyber incidents.
11 December 2020	The Bill was referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for review.	The PJCIS received 75 submissions, and released an Advisory Report recommending that the Bill be split so that elements of it could be passed before the next Federal election.
March 2021	Consultation on risk management program rules.	The department hosted four town hall forums and seven workshops to develop risk management program rules.
23 April 2021	Consultation paper released on draft Critical Infrastructure Asset Definition Rules.	Proposed rules for those asset classes that would be subject to the amended regulatory framework.
29 September 2021	PJCIS advisory report released on amendments to the SoCI Act.	The report made 14 recommendations, including that the Bill be split in two to allow urgent elements to be legislated (Bill 1) and remaining elements to undergo further consultation (Bill 2). Urgent elements referred to in the review report were government assistance measures in proposed Part 3A, and the definitions and meanings of expanded critical infrastructure sectors and assets.
22 November 2021	<i>Security Legislation Amendment (Critical Infrastructure) Act 2021</i> (the SLACI Act) passed by Parliament.	<p>Bill 1 of amendments to the <i>Security of Critical Infrastructure Act 2018</i> (SoCI Act) included:</p> <ul style="list-style-type: none"> • expansion of scope from four to eleven sectors; • government assistance measure; • cyber security reporting obligations; and • expanded reporting requirements for critical infrastructure operators and owners.
15 December 2021	Public consultation commenced on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022.	<p>Bill 2 of amendments to the SoCI Act included:</p> <ul style="list-style-type: none"> • the Risk Management Program; • enhanced cyber security obligations; • Systems of National Significance; and • information sharing provisions for regulated entities.
February 2022	The PJCIS published its report on the statutory review of Part 14 of the	The Committee made six recommendations. It recommended:

Date	Event	Event consequences
	<i>Telecommunication Act 1997</i> ^c	'that the Department of Infrastructure, Transport, Regional Development and Communications do an environmental analysis of the current national and international telecommunications markets and networks, in tandem with the Cyber and Infrastructure Security Centre (CISC) in the Department of Home Affairs, to identify industry best practice risk identification, management and mitigation... This analysis can then feed into the development of industry rules and obligations within the expanded SOCI Bill to be introduced in the future, as well as identify better guidelines, support tools, and standards to be applied to project notification, assessment and development of security capability plans.' ^d
25 March 2022	The PJCIS published its Advisory Report on the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022.	The Committee made 11 recommendations, which aimed to ensure that: <ul style="list-style-type: none"> • the cooperative relationship with industry can continue to inform the flexible regulatory base that the Bill proposes; • the Committee is notified when sensitive powers are exercised and that consultation is ongoing and effective; • elements of the potential impact of the Bill on workers' rights are clarified, definitions codified and that review mechanisms be considered; and • the Bill's mechanisms will be reviewed for their effectiveness, operation and proportionality, once the new powers are finalised and implemented.
31 March 2022	Security Legislation Amendment (Critical Infrastructure Protection) Bill passed by Parliament.	Bill 2 of amendments to the SoCI Act included: <ul style="list-style-type: none"> • Risk Management Program requiring critical infrastructure owners and operators to manage the risk of hazards that affect the delivery of essential services; designed with industry and building on existing regulatory frameworks, where possible. • the ability to declare Systems of National Significance — the most interconnected and interdependent of our critical infrastructure assets. • enhanced Cyber Security Obligations for owners and operators of assets most critical to the nation (the systems of national significance) — centred around a strengthened relationship with government. • improved information sharing provisions to make it easier for regulated entities and governments to share information as needed to comply with their obligations.

Note a: Available from <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf> [accessed on 4 January 2022].

Note b: Department of Home Affairs, *Australia's Cyber Security Strategy 2020 [Internet]*, DHA, 2020, pp.28–29, Available from <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australia%E2%80%99s-cyber-security-strategy-2020> [accessed on 20 December 2021].

Note c: Parliament of Australia, *Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms [internet]*, APH, available from Review of Part 14 of the Telecommunications Act 1997 – Telecommunications Sector Security Reforms (aph.gov.au) [accessed on 21 March 2022].

Note d: *ibid.*, p.44.

Source: ANAO analysis of departmental documentation.

Appendix 4 Other jurisdiction critical infrastructure arrangements

1. Tables A.2 to A.6 provide non-exhaustive comparisons of key characteristics of the critical infrastructure programs in Australian jurisdictions.

Table A.2: Key enabling legislation for critical infrastructure programs in Australian jurisdictions

Jurisdiction	Key enabling legislation
Australian Government	<i>Australian Securities and Investments Commission Act 2001</i> <i>Business Names Registration Act 2011</i> <i>Corporations Act 2001</i> <i>Foreign Acquisitions and Takeovers Acquisition Act 1975</i> <i>Infrastructure Act 2018</i> <i>Insurance Contracts Act 1984</i> <i>Maritime Transport and Offshore Facilities Security Act 2003</i> <i>National Consumer Credit Protection Act 2009</i> <i>National Electricity Law</i> <i>National Energy Retail Law</i> <i>National Gas Law</i> <i>Offshore Electricity Infrastructure Act 2021</i> <i>Shipping Registration Act 1981</i> <i>Security of Critical Aviation Transport Security Act 2004</i> <i>Telecommunications Act 1997</i> <i>Telecommunications (Interception and Access) Act 1979</i>
Australian Capital Territory	<i>Emergencies Act 2004</i> <i>Water Resources Act 2007</i>
New South Wales	<i>Dangerous Goods (Road and Rail Transport) Act 2008 No 95</i> <i>Dams Safety Act 2015</i> <i>Electricity Supply Act 1995</i> <i>Essential Services Act 1988</i> <i>Gas Supply Act 1996</i> <i>Heavy Vehicle National Law (NSW) and Regulations</i> <i>Independent Pricing and Regulatory Tribunal Act 1992</i> <i>Marine Safety Act 1998</i> <i>Natural Resources Access Regulator Act 2017</i> <i>Passenger Transport Act 1990</i> <i>Passenger Transport Act 2014</i> <i>Ports and Maritime Administration Act 1995</i> <i>Rail Safety (Adoption of National Law) Act 2012</i> <i>Rail Safety National Law (NSW)</i> <i>Roads Act 1993</i> <i>Road Transport Act 2013 No 18</i> <i>State Emergency and Rescue Management Act 1989</i>

Jurisdiction	Key enabling legislation
	<i>Transport Administration Act 1988</i> <i>Water Act 1912</i> <i>Water Management Act 2000</i> <i>Water NSW Act 2014</i> <i>Water Supply (Critical Needs) Act 2019</i>
Northern Territory	<i>Electricity Reform Act</i> <i>Ports Management Act 2015</i> <i>Water Supply and Sewerage Services Act</i>
Queensland	<i>Disaster Management Act 2003</i> <i>Transport Infrastructure Act 1994</i> <i>Transport Operations (Maritime Safety) Act 1994</i>
South Australia	<i>Emergency Management Act 2004</i> <i>Electricity Act 1996 (SA)</i> <i>Essential Services Commission Act 2002 (SA)</i> <i>Maritime Services (Access) Act 2000</i>
Tasmania	<i>Emergency Management Act 2006</i>
Victoria	<i>Electricity Industry Act 2000</i> <i>Emergency Management Act 2013</i> <i>Emergency Management (Critical Infrastructure Resilience) Regulations 2015</i> <i>Marine Safety Act 2010</i> <i>Port Management Act 1995</i> <i>Terrorism (Community Protection) Act 2003</i> <i>Transport Integration Act 2010</i>
Western Australia	<i>Emergency Management Act 2005</i> <i>Port Authorities Act 1999</i> <i>State Emergency Management Regulations 2006</i>

Source: ANAO analysis of information available in the public domain.

Table A.3: Key critical infrastructure program policies in Australian jurisdictions

Jurisdiction	Key critical infrastructure-related policies
Australian Government	Australia's Cyber Security Strategy (2020) Australian Government Crisis Management Framework Critical Infrastructure Resilience Strategy (2015) National Disaster Risk Reduction Framework (2020) National Guidelines for Protecting Critical Infrastructure from Terrorism (2015)
Australian Capital Territory	Protective security, crime prevention, business continuity and risk management, and emergency management strategies.
New South Wales	NSW Critical Infrastructure Resilience Strategy — Partner, Prepare, Provide (2018) Regional Disaster Preparedness Program

Jurisdiction	Key critical infrastructure-related policies
	State Level Emergency Risk Assessment (2017)
Northern Territory	Protective security, crime prevention, business continuity and risk management, and emergency management strategies Territory Emergency Management Council Strategic Plan 2020–2023
Queensland	Emergency Management Assurance Framework. Protective security, crime prevention, business continuity and risk management, and emergency management strategies Queensland Strategy for Disaster Resilience (2017) Queensland Disaster Management Queensland State Disaster Management Plan Strategic Policy Statement
South Australia	Protective security, crime prevention, business continuity and risk management, and emergency management strategies SA 2020 Risks and Hazards summary State Emergency Management Plan
Tasmania	Protective security, crime prevention, business continuity and risk management, and emergency management strategies Tasmanian Disaster Resilience Strategy 2020–2025
Victoria	All Sectors Resilience Reports Critical Infrastructure Resilience Interim Strategy (December 2013) Critical Infrastructure Resilience Strategy (2016) Emergency Management Manual Victoria Ministerial Guidelines (2017) Roadmap for Victorian Critical Infrastructure Resilience (December 2012) Victorian Emergency Management Reform White Paper
Western Australia	State Emergency Management (EM) Framework State EM Plan State EM Policy State EM Procedures

Source: ANAO analysis of information available in the public domain.

Table A.4: Critical infrastructure policy leads in Australian jurisdictions

Jurisdiction	Critical infrastructure policy leads in Australian jurisdictions
Australian Government	Australian Taxation Office Department of Agriculture, Water and the Environment Department of Defence Department of Education, Skills and Employment Department of Health Department of Home Affairs Department of Industry, Science, Energy and Resources

Jurisdiction	Critical infrastructure policy leads in Australian jurisdictions
	Department of Infrastructure, Transport, Regional Development and Communications Department of the Treasury Reserve Bank of Australia
Australian Capital Territory	Access Canberra Chief Minister, Treasury and Economic Development Directorate Emergency Services Agency Territory directorates responsible for each critical infrastructure sector
New South Wales	Cyber NSW Department of Premier and Cabinet NSW Resilience NSW State portfolio departments responsible for each critical infrastructure sector
Northern Territory	Department of the Chief Minister and Cabinet Territory departments responsible for each critical infrastructure sector
Queensland	Department of the Premier and Cabinet Queensland Bulk Water Supply Authority
South Australia	Department of the Premier and Cabinet State portfolio departments responsible for each critical infrastructure sector
Tasmania	Department of Premier and Cabinet State portfolio departments responsible for each critical infrastructure sector
Victoria	Department of Premier and Cabinet Emergency Management Victoria State portfolio departments responsible for each critical infrastructure sector
Western Australia	Department of the Premier and Cabinet State portfolio departments responsible for each critical infrastructure sector

Source: ANAO analysis of information available in the public domain.

Table A.5: Key critical infrastructure-related incident response entities in Australian jurisdictions

Jurisdiction	Key critical infrastructure-related incident response entities
Australian Government	Australian Communications and Media Authority Australian Energy Market Organisation Australian Federal Police Australian Maritime Safety Authority Australian Security Intelligence Organisation Australian Signals Directorate Department of Health
Australian Capital Territory	ACT Health ACT Police Emergency Services Agency

Jurisdiction	Key critical infrastructure-related incident response entities
New South Wales	Cyber NSW NSW Health NSW Police Force Resilience NSW
Northern Territory	NT Police, Fire and Emergency Services
Queensland	Queensland Fire and Emergency Services Queensland Police
South Australia	Country Fire Service Department of Planning, Transport and Infrastructure Department of the Premier and Cabinet Primary Industries and Regions SA SA Health South Australia Police
Tasmania	Tasmania Police
Victoria	Emergency Management Victoria Inspector General for Emergency Management Victoria Police Victorian Ports Corporation
Western Australia	Department of the Premier and Cabinet Police Force of Western Australia

Source: ANAO analysis of information available in the public domain.

Table A.6: Key critical infrastructure government regulators in Australian jurisdictions

Jurisdiction	Key critical infrastructure government regulators
Australian Government	Australian Communications and Media Authority Australian Energy Market Commission Australian Energy Market Operator Australian Energy Regulator Australian Maritime Safety Authority Australian Prudential Regulation Authority Australian Securities and Investment Commission Department of Industry, Science, Energy and Resources Department of the Treasury Food Standards Australia and New Zealand National Offshore Petroleum Safety and Environmental Management Authority
Australian Capital Territory	Chief Minister, Treasury and Economic Development Directorate Territory directorates responsible for each critical infrastructure sector
New South Wales	Department of Planning and Environment Independent Pricing and Regulatory Tribunal

Jurisdiction	Key critical infrastructure government regulators
	Port Authority of New South Wales
Northern Territory	Territory departments responsible for each critical infrastructure sector Utilities Commission
Queensland	Department of Energy and Water Supply Department of Transport and Main Roads
South Australia	Essential Services Commission Office of the Technical Regulator
Tasmania	Office of the Tasmanian Economic Regulator
Victoria	Department of Environment, Land, Water and Planning Essential Services Commission
Western Australia	Department of Transport Economic Regulation Authority.

Source: ANAO analysis of information available in the public domain