COUNTRY: **AUSTRALIA**

Legal Foundations: Australia's national cybersecurity strategy was adopted in 2009 and is currently under review. A revised strategy is expected to be released in late 2015. While Australia has a strong legal framework for information classification, it enacts its information security through guidelines and similar policy documents as opposed to acts of Parliament, and there is no dedicated information security act or classified information act.

Operational Entities: The Australian Cyber Security Centre, launched in 2014, is a hub bringing together the numerous agencies that are engaged with cybersecurity and information security; however, there remains some confusion regarding the separation of responsibilities. Both CERT Australia and the Australian Signals Directorate operate incident-reporting services.

Public-Private Partnerships: Australia does not have a formal public-private partnership for cybersecurity, however CERT Australia works with the private sector in awareness programs and critical infrastructure protection. The private sector also has been consulted as part of the cybersecurity strategy review process.

Sector-Specific Cybersecurity Plans: There is no joint public-private sector plan in Australia that addresses cybersecurity. The Critical Infrastructure Resilience Strategy does highlight the participation of "sector groups" as a key part of the Trusted Information Sharing Network (TISN), but the TISN was not intended to produce sector-specific plans.

Education: Australia has a comprehensive cybersecurity education strategy in place for all age groups, and has heavily invested in education materials and initiatives.

Additional Cyberlaw Indicators: Australia is largely free of country-specific restrictions on technology providers (e.g., mandatory technology requirements, local testing requirements, and requirements for the sharing of source code), but some restrictions and burdens do exist in the procurement space.

	QUESTION	RESPONSE	EXPLANATORY TEXT
	LEGAL FOUNDATIONS		
1.	Is there a national cybersecurity strategy in place?	✔	The Cyber Security Strategy <www.ag.gov.au/RightsAndProtections/CyberSecurity> was adopted by the Australian Government in 2009. The strategy includes a statement of guiding principles, an assessment of stakeholders involved, and clearly stated objectives attached to a loose implementation timeline. The assessment of Australia's cybersecurity capacity and strength of its legal framework is limited. The Australian Cyber Security Strategy is the subject of a review by the Department of Prime Minister and Cabinet and is expected to be updated in late 2015 <www.dpmc.gov.au/pmc/about-pmc/core-priorities/national-security-and-international-policy/australian-governments-cyber-security-review>.
2.	What year was the national cybersecurity strategy adopted?	2009	
3.	Is there a critical infrastructure protection (CIP) strategy or plan in place?	✔	Pursuant to the proposals of the Cyber Security Strategy <www.ag.gov.au/RightsAndProtections/CyberSecurity>, the Critical Infrastructure Resilience Strategy <www.tisn.gov.au> was published in 2010.
4.	Is there legislation/policy that requires the establishment of a written information security plan?	◑	There is no legislation in place in Australia that requires the establishment of a written information security plan. Australia has developed the Protective Security Policy Framework (PSPF) <www.protectivesecurity.gov.au>, which includes the Information Security Management Guidelines <protectivesecurity.gov.au/informationsecurity>, approved by the Attorney-General's Department <www.agd.gov.au>, and an information security management protocol <www.protectivesecurity.gov.au/informationsecurity> that outlines the information security practices and procedures for employees of government agencies.

COUNTRY: AUSTRALIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
5.	Is there legislation/policy that requires an inventory of "systems" and the classification of data?	✔	The Information Security Management Guidelines <protectivesecurity.gov.au/informationsecurity>, approved by the Attorney-General's Department <www.agd.gov.au> in 2010 and last amended in 2015, require information to be classified if disclosure of that information would be a detriment to Australia's interests. The criteria for determining this is set out in Section 3 of the guidelines. The classification system is four-tiered, and classification levels are assigned according to the level of risk involved in disclosing the information.
6.	Is there legislation/policy that requires security practices/ requirements to be mapped to risk levels?	✔	Security practices for government information, both sensitive and non-sensitive, are mapped to assigned classification levels, as outlined in the Information Security Management Guidelines <protectivesecurity.gov.au/informationsecurity>. These classification levels are assigned according to the risk level involved in disclosing the information.
7.	Is there legislation/policy that requires (at least) an annual cybersecurity audit?	✖	There is no legislation or policy in place in Australia that requires at least an annual cybersecurity audit. The Australian Signals Directorate (ASD) <www.asd.gov.au> and the Australian Government Information Management Office (AGIMO) <www.finance.gov.au/agimo> jointly run OnSecure, a database of information security event reports and their analysis. However, the data and analysis on OnSecure is not the product of an audit process. OnSecure is disseminated online to all government agencies.
8.	Is there legislation/policy that requires a public report on cybersecurity capacity for the government?	◑	There is no legislation in place in Australia that requires a public report on cybersecurity capacity for the government. However, the Cyber Security Strategy released in 2009, the Critical Infrastructure Resilience Strategy <www.tisn.gov.au> released in 2010, and the 2013 Defence White Paper <www.defence.gov.au/WhitePaper2013> include limited assessments of Australia's cybersecurity capacity. All three reports are publicly available. The Australian Cyber Security Strategy is the subject of a review by the Department of Prime Minister and Cabinet and is expected to be updated in 2015 <https://www.pm.gov.au/media/2014-11-27/cyber-security-review-0>.
9.	Is there legislation/policy that requires each agency to have a chief information officer (CIO) or chief security officer (CSO)?	✔	The Protective Security Policy Framework (PSPF) <www.protectivesecurity.gov.au>, which includes the Information Security Management Guidelines <protectivesecurity.gov.au/informationsecurity>, requires each government entity to establish a security executive. The Information Security Manual 2015 <www.asd.gov.au/infosec/ism> requires a member of the executive to be appointed the Chief Information Security Officer.
10.	Is there legislation/policy that requires mandatory reporting of cybersecurity incidents?	✔	The Australian Signals Directorate's (ASD) <www.asd.gov.au> Information Security Manual 2015 <www.asd.gov.au/infosec/ism> requires that government entities report cybersecurity incidents and notes that mandatory retention of records such as event logs and audit trails for specific minimum periods are required by the Archives Act 1983 <www.comlaw.gov.au/Series/C2004A02796>.
11.	Does legislation/policy include an appropriate definition for "critical infrastructure protection" (CIP)?	✔	The Critical Infrastructure Resilience Strategy <www.tisn.gov.au> includes an appropriate definition for "critical infrastructure protection".
12.	Are requirements for public and private procurement of cybersecurity solutions based on international accreditation or certification schemes, without additional local requirements?	✔	The Australian Cyber Security Strategy 2009 <www.ag.gov.au/RightsAndProtections/CyberSecurity> includes a commitment to review the Australian Government's Protective Security Manual <www.protectivesecurity.gov.au> to "ensure that its information security policies and standards continue to keep pace with developments in technology and reflect international best practice. The aim of this review will be to, wherever practicable, link Australian Government requirements to corresponding commercial standards to promote the adoption of similar best practice approaches across the private sector." The strategy also promotes international engagement, including the promotion of international standards.
	OPERATIONAL ENTITIES		
1.	Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?	✔	CERT Australia <www.cert.gov.au> was established in 2010. It is responsible for coordinating security and incident response measures for networks used by entities engaged with critical infrastructure as well as systems of national interest. A definition for "systems of national interest" is included in the Cyber Security Strategy <www.ag.gov.au/RightsAndProtections/CyberSecurity>.
2.	What year was the computer emergency response team (CERT) established?	2010	

COUNTRY: AUSTRALIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
3.	Is there a national competent authority for network and information security (NIS)?	✔	Australia has multiple agencies that are responsible for the management of network and information security: • The Australian Cyber Security Centre (ACSC) <www.acsc.gov.au> is a hub that brings together relevant government departments and law enforcement agencies. • The Australian Signals Directorate (ASD) <www.asd.gov.au> is the authority responsible for the security of information and communications technology for government agencies and departments, including providing oversight for information security management. It is the agency that chiefly manages the ACSC. • The Australian Security Intelligence Organisation (ASIO) <www.asio.gov.au>, an Australian intelligence service, is responsible for responding to cybersecurity incidents which are deemed to be related to espionage, sabotage, terrorism, or other forms of politically related violence. • In addition to ASIO, the Australian Federal Police (AFP) <www.afp.gov.au> may be involved as part of an investigation and analysis process. The Joint Operating Arrangements (JOA), as outlined in the Cyber Security Strategy <www.ag.gov.au/RightsAndProtections/CyberSecurity>, is a process whereby the three key agencies (ACSC, ASD, and ASIO) identify and analyze an information security incident and determine which agency has the primary responsibility to enact security response procedures for that incident. In addition to the agencies above, the Australian Government Information Management Office (AGIMO) <www.finance.gov.au/agimo> is the agency responsible for developing and implementing information and communications technology.
4.	Is there an incident-reporting platform for collecting cybersecurity incident data?	✔	CERT Australia <www.cert.gov.au> is tasked with collecting information about cybersecurity incidents. They engage proactively by monitoring their constituency for cyber incidents, as well as having in place an online and telephone reporting structure to log cybersecurity incidents. In addition to CERT Australia, the Australian Signal Directorate (ASD) <www.asd.gov.au> maintains an incident-reporting platform which includes an online form and telephone support.
5.	Are national cybersecurity exercises conducted?	◑	Australia has participated in multi-national cybersecurity exercises organized by the United States.
6.	Is there a national incident management structure (NIMS) for responding to cybersecurity incidents?	✔	Incident management procedures are covered in both the Cyber Security Strategy <www.ag.gov.au/RightsAndProtections/CyberSecurity>, the Information Security Management Guidelines <protectivesecurity.gov.au/informationsecurity>, and the Australian Signals Directorate's Information Security Manual 2015 <www.asd.gov.au/infosec/ism>. These include processes and controls that cover the reporting and handling of cybersecurity incidents by government agencies.
	PUBLIC-PRIVATE PARTNERSHIPS		
1.	Is there a defined public-private partnership (PPP) for cybersecurity?	✖	There is no defined public-private partnership for cybersecurity in Australia. CERT Australia <www.cert.gov.au> liaises with the private sector in its role as coordinator of incident response measures. Furthermore, the Australian Cyber Security Centre (ACSC) is expected to work in close cooperation with the private sector.
2.	Is industry organized (i.e., business or industry cybersecurity councils)?	◑	There is no industry-led platform dedicated to cybersecurity issues in Australia. The Australian Computing Society (ACS) <www.acs.org.au> and the Australian Information Industry Association (AIIA) <www.aiia.com.au> are two representative associations for the Australian information and communication technology sector. The ACS and AIIA engage with cybersecurity issues in the course of their duties. Also active in this area is the Australian Information Security Association (AISA) <www.aisa.org.au>, a representative body for Australian information security professionals.
3.	Are new public-private partnerships in planning or underway (if so, which focus area)?	✖	As of May 2015, there are no documented new public-private partnerships being planned in Australia.

COUNTRY: AUSTRALIA

	QUESTION	RESPONSE	EXPLANATORY TEXT
	SECTOR-SPECIFIC CYBERSECURITY PLANS		
1.	Is there a joint public-private sector plan that addresses cybersecurity?	◑	There is no joint public-private sector plan in Australia that addresses cybersecurity. The Critical Infrastructure Resilience Strategy <www.ag.gov.au/NationalSecurity/InfrastructureResilience/Pages/default.aspx> does highlight the participation of "sector groups" as a key part of the Trusted Information Sharing Network (TISN) <www.tisn.gov.au>, however the TISN was not intended to produce sector-specific plans.
2.	Have sector-specific security priorities been defined?	✖	Sector-specific security priorities have not been publicly defined, nor has there been a proposal to define sector-specific security priorities in legislation or policy as of May 2015.
3.	Have any sector cybersecurity risk assessments been conducted?	✖	Sector cybersecurity risk assessments have not been conducted. General risk assessment for the critical infrastructure sector are proposed in the Critical Infrastructure Resilience Strategy <www.tisn.gov.au>, which does address the involvement of "sector groups."
	EDUCATION		
1.	Is there an education strategy to enhance cybersecurity knowledge and increase cybersecurity awareness of the public from a young age?	✔	Australia has a comprehensive cybersecurity education strategy in place for all age groups and has invested heavily in education materials and initiatives, including: • Cybersmart; • Stay Safe Online; • The Cybersafety Help Button; and • The Budd: e Cybersecurity Builder These materials are all available from a central cybersecurity education portal <australia.gov.au/topics/it-and-communications/cyber-security>.
	ADDITIONAL CYBERLAW INDICATORS		
1.	Are cybersecurity services able to operate free from laws that discriminate based on the nationality of the vendor?	◑	Cybersecurity services may be subject to government and agency procurement policies that encourage the involvement of local SMEs (for example the State of Victoria requires a 40% local component in some strategic project tenders, and the State of New South Wales applies a 20% price preference margin to local suppliers for some government projects). Australia is an observer, but not a full member, of the WTO plurilateral Agreement on Government Procurement. The European Union has noted: "Australia is the only major industrialized country which has not joined the WTO plurilateral agreement on Government Procurement." [European Union Trade Directorate, Australia - Government procurement, 2009, <madb.europa.eu/madb/barriers_details.htm?barrier_id=095278&version=5>]
2.	Are cybersecurity services able to operate free from laws or policies that mandate the use of specific technologies?	✔	There are no mandatory technology requirements in Australian law and policy.
3.	Are cybersecurity services able to operate free from additional local testing requirements that go beyond international testing requirements?	✔	There are no local testing requirements for cybersecurity services as of May 2015.
4.	Are cybersecurity services able to operate free from laws or policies that mandate the submission of source code or other proprietary information?	✔	There are no local requirements for the submission of source code in relation to cybersecurity services as of May 2015.
5.	Are cybersecurity services able to operate free from laws or policies that require service providers to locate their servers inside the subject country?	◑	There are no specific requirements for servers to be located in Australia, however some government outsourcing and offshoring arrangements are subject to an extra layer of "approval" by senior officials if the data is to be located offshore. The approval process must balance national security risks against other benefits.
6.	Are cybersecurity services able to operate free from unnecessary restrictions on cross-border data flows (such as registration requirements)?	✔	There are no registration requirements in Australia. The privacy law does include some basic, light-touch, cross-border transfer rules.