Global Information Assurance Certification Paper

A CONCISE GUIDE TO VARIOUS AUSTRALIAN LAWS RELATED TO PRIVACY AND CYBERSECURITY DOMAINS

GIAC GLEG Gold Certification

Author: Babu Veerappa Srinivas, babuseenu@gmail.com
Advisor: Barbara L. Filkins

Accepted: June 15, 2015

Abstract

There are many laws in Australia related to privacy and cyber security domains. In this paper, the author intends to collate the current laws related to privacy and cyber security domains so that interested readers could get relevant information specific to Australia in one concise document. Additionally, there are no industry specific acts or regulations like HIPAA, SOX or GLBA. Because of this, some organizations do not know their obligations in relation to these laws.

This paper presents research on the current applicable cyber security related laws, Acts and regulations published by the Federal and State Governments, established relationship with other applicable Acts, performed a gap assessment and identified relevant industry frameworks that can be adopted as best practices. For ease of future research, the source of these current artefacts and database are cited for throughout the document.

Disclaimer: Contents of this document must not be construed as legal advice. Readers are encouraged to seek legal advice prior to consideration.

1. Introduction

1.1. Preamble

Organizations do not like to be in the front page headline of the newspapers due to a cyber-security breach. To be the good cyber netizen, most do the right things by implementing layered defenses using different cyber security controls. The objective of such activity is to either thwart or minimize cyber intrusions. These controls might be based on industry best practices like the National Institute of Standards and Technology NIST SP-800 publications (CSRC, 2015), Centre for Internet Security benchmarks (CISecurity, 2015) or best practices published by vendors like Cisco (Cisco, 2015), Microsoft (Microsoft, 2015), IBM (IBM, 2015), and Oracle (Oracle, 2015). As a best practice, some may choose standards such as ISO 27002 (ISO, 2015) which is a generic Information Security Management System (ISMS) or a specific standard like Payment Card Industry – Data Security Standard (PCI, 2015).

Implementing security controls costs money. Such costs vary from industry to industry and organization to organization. Due to this, the degree and depth of implementation of such controls varies. Most organizations treat the security department and its activities as a cost center rather than a business enabler. An organization that treats security as a business enabler might have the right security controls to minimise most risks posed by various cybersecurity threats (Wisseman, 2015). On the other hand, an organization that sees security as a cost center might not allocate enough budget to protect its business. For such organizations, this may lead to unintended cyber security breaches that results in impacts such as loss of customer data, reputation damage, loss of revenue, interruption to business and legal consequences.

Since organizations apply discretion in security spending, one way to force them to take the right action is to mandate compliance with a legislative or regulatory framework. Such frameworks provide confidence (Greenwald, 2015) to the general public and/or the organizational stakeholders who either depend on such organizations for their benefit or to minimize the supply-chain risk (Wilkerson, 2014). In the current cyber-connected world, it is important to note the fact (*Cyber-security risks in the supply*

chain, 2015) that the perpetrators prey on upstream or downstream supply-chain provider of an organization to commit cybersecurity breach. Hence it is important for these supply-chain providers to be aware of their legal and regulatory obligations.

In the event of a cyber-security breach, one of the key impacts to an organization is the legal consequences (Germano & Goldman, 2014). This could make or break an organization if it is caught off-guard in its compliance with legal, legislative or regulatory obligations. Hence such organizations would like to be in a position to prove to the law enforcement agencies that they complied with the relevant legislation or a regulation. The first step in this journey is for senior management to understand the legal and regulatory requirements and obligations.

There are various discussions across the globe about the advantages and disadvantages of enforceable regulatory arrangements versus voluntary, self-regulation and industry guidelines to support improved control of cyber security. This paper does not address such pros and cons; instead its focus is to provide some information on the obligations imposed by various regulatory and legislative authorities within the Commonwealth of Australia. Further this document also covers artefacts from some of the key voluntary and self-regulated governing bodies.

1.2. Document Coverage

This document collates many of the cybersecurity-related legal and regulatory requirements of the Federal Government of Australia, known to the author at the time of writing this paper Some of the state-specific (Victoria and South Australia) requirements are also documented for the readers to provide an insight how some of the state and federal laws differ. For certain domains, such as Privacy Laws, there could be both state and federal laws that apply to an organization operating in a particular state. Readers are advised to compare both laws and comply with the one that is broader and restrictive than the other so that there is adequate coverage of both laws.

The current legal and regulatory environment in Australia is briefly covered in Section 2. Readers can quickly look at Table 1 and ascertain whether a particular regulatory obligation applies or a relevant voluntary guideline is the answer for adopting

good practices in cybersecurity domain. This section also summarises the various federal and state legislation database for the convenience of the reader.

Common legislative obligations apply to most of the government agencies and private organizations. Other complimentary legislative Acts for the four key obligations are summarised in this section. Those obligations and their source are documented in Table 2 in Section 3.

Voluntary guidelines for the key industry verticals and government agencies, nine in total, are documented in Section 4. Readers are reminded that they are required to do due diligence before adopting these guidelines.

Section 5 wraps up the paper highlighting the importance of compliance with regulatory obligations and benefits of adoption of voluntary cybersecurity related guidelines. A few topics for further research in this domain are also highlighted.

2. The Legal, Legislative and Regulatory Environment

The key question most of the organizations, security practitioners and legal counsels in Australia should ask is whether they have enough guidance either from the state or the federal government pertaining to an organization's cybersecurity obligations. If the answer is "yes", what is the guidance? If "no", where can this information be found?

The popular industry and government sectors in Australia were analyzed against the available cybersecurity related voluntary guidance, laws, regulation and legislation and a summarized version of the findings is presented in Table 1. The first column identifies the industry sector and the next column provides brief commentary about the supporting cyber security guidance artefacts. Interested readers can use this table as a starting point in their understanding of applicable guidance for a particular sector. More information on these artefacts are documented in the further sections of this paper.

It must be noted that there are a few cyber security related legal, legislative and regulatory obligations applicable for all industry sectors including government agencies. Table 1 highlights the specific artefact that applies to a sector other than the common

obligations listed here. The artefacts that commonly apply to all private organizations and government agencies are:

- Australian Privacy Principles (APP) – The new APPs are part of the amendment to Privacy Act 1988 (Cth) which has ended the complexity and confusion in the applications of privacy laws by creating a set of APPs that will apply to both federal government agencies and private sector organizations. These APPs will regulate the collection, holding, use and disclosure of personal information that is included in records. They apply to government and private organizations having more than $3 AUD million annual turnover.
- Cybercrime Act – This Act offers more comprehensive regulation of computer and Internet related offences such as unlawful access and computer trespass, damaging data and impeding access to computers, theft of data, computer fraud, cyber-stalking and harassment and possession of child pornography. It created a number of investigation powers and criminal offenses designed to protect the security, reliability, and integrity of computer data and electronic communications. Further, it enhances the applicability of the existing search-and-seizure provisions relating to electronically stored data.
- Spam Act – This Act establishes a scheme for the regulation of commercial email and other types of electronic messages. It restricts unauthorized, unsolicited electronic messages with some exemptions. Rules for consent, identification of the sender and the unsubscribe features are explained in this Act. This Act is regulated by the "Australian Communications and Media Authority."
- Telecommunications (Interception and Access) Act – The primary objective of this Act is to protect the privacy of individuals who use the Australian telecommunication systems. Another purpose is to specify the circumstances under which it is lawful for interception of, or access to, communications to take place. This Act covers both stored and real time communications.

Principle 7 of Australian Stock Exchange (ASX) "Corporate Governance Principles and Recommendations" applies to all organizations listed in the Exchange.

Similarly some artefacts from Australian Prudential Regulatory Authority (APRA) apply to banking and financial sector organizations. Additionally organizations that process credit card information are obligated to comply with Payment Card Industry – Data Security Standard (PCI-DSS) as mandated by the respective payment gateways. This includes charities who accept donations via credit cards. With minor modifications organizations that fall under the critical infrastructures category can use Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) as a good framework to improve cybersecurity posture.

Table 1 -- Summary of Applicability

Sector	Commentary
Banking and Finance	APRA CPG 235 and PPG 234, relevant sub sections of section RG104 of AFSL license obligation (RG 104.93 and RG 104.96). Additionally recommended to follow ISO 27001/2, and COBIT 5.
Federal Government	Australian Government Protective Security Policy Framework (PSPF) and Information Security Manual (ISM)
Healthcare Providers	Royal Australian College of General Practitioners (RACGP) Computer and Information Security Standards, National Health and Medical Research Council's "The regulation of health information privacy in Australia". Additionally recommended to follow ISO 27001/2, and COBIT 5.
Internet Service Providers	Communications Alliance C650:2014 icode, Australian Communications and Media Authority's "Australian Internet Security Initiative" (ACMA, 2015), Telecommunications (Interception) and Listening Device Amendment Act. Additionally recommended to follow ISO 27001/2, and COBIT 5.
Manufacturing	None, recommended to follow ISO 27001/2, and COBIT 5

Sector	Commentary
Mining	None, recommended to follow ISO 27001/2, ISO 27019 and COBIT 5
Retailers	None, recommended to follow ISO 27001/2, and COBIT 5
State Government	None, but increasingly various states are using PSPF and ISM and the baseline. Readers much check their particular state's requirement published by the state government.
Telecommunications Providers	Telecommunications (Interception) and Listening Device Amendment Act, Australian Communications and Media Authority's "Australian Internet Security Initiative" (ACMA, 2015). Additionally recommended to follow ISO 27001/2, and COBIT 5.
Utilities	None, recommended to follow ISO 27001/2, ISO 27019, COBIT 5 and NERC-CIP V5

Upon a review of the current published cybersecurity-related laws and regulations, it is evident that Australia has a few general cybersecurity related laws but is missing some of the industry specific regulations. Examples of missing regulatory frameworks are ones similar to the United States Health Insurance Portability and Accountability Act (HIPAA) and North American Energy Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) controls.

For those missing regulatory frameworks in Australia, it is a recommended practice for the Australian organizations to adopt some of the regulatory frameworks from the United States (US) or Europe. This will provide a good head-start if such regulatory frameworks are mandated in the near future. One such example is the recommendation (ASIC, 2015) of the Australian Securities and Investment Corporation's (ASIC) advice to adopt NIST Cyber Security Framework for Critical Infrastructure by organizations listed in the ASX. Similarly, adoption of NERC-CIP framework by the Australian energy suppliers can provide these suppliers an advantage over others who do

not, if compliance with a regulatory framework is ever mandated by the Australian Energy Regulator (AER).

Since the cyber threats are evolving rapidly (Verizon, 2015) and affecting every industry and government sector, the regulatory or the governing bodies are investing time and efforts in publishing latest guidance related to cyber security. Readers of this document are encouraged to research specific guidance and obligations imposed by their relevant governing authority for the latest information.

3. Common Legislative Obligations

Most developed nations have some sort of cybersecurity strategy (*Cybersecurity policy making at a turning point*, 2012) in place. This emphasizes that there are some legislative and regulatory obligations that expect behaviour of each in cyberspace. This in turn provides confidence to the stakeholders and government that the organizations act diligently to safeguard sensitive data and personal information. This section documents some of the common legislative and regulatory frameworks that are obligated upon the government and private business in Australia.

3.1. Privacy Act 1988 (Cth) and its Australian Privacy Principles

This federal Privacy Act and its associated Privacy Principles apply to all government agencies and private sector entities with an annual turnover of at least three million Australian dollars. The private sector entities can be an individual, body corporate, partnership, a trust or an unincorporated association. This Act has significantly strengthened the powers of the Privacy Commissioner in relation to imposing fines (up to $1.7 million AUD for organizations and up to $340,000 AUD for individuals) for serious Privacy Act breach and to conduct independent investigation.

In the context of this federal Act, Personal Information (Personal Data) means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in material form or not. Sensitive Information (Personal Data) means information or an opinion about health information, criminal record, sexual orientation, religious beliefs, racial or ethnic origin, biometric information

and /or genetic information. There are specific rules defined on how personal and sensitive information can be collected, processed and/or transferred to other entities. Although breach notification is ***not mandatory,*** the Office of the Australian Information Commissioner (OAIC) has released guidance on how and when to release breach notification. As a best practice OAIC highly recommends to follow data breach notification guidelines. The Australian Law Reform Commission (ALRC) has recommended that the Privacy Act be amended to impose a mandatory obligation to notify the Privacy Commissioner and affected individuals in the event of a data breach that could give rise to a real risk of serious harm to affected individuals. Readers of this paper should keep an eye on the future changes in breach reporting obligations.

Most of the states and territories have their own data protection legislation applying to both State Government agencies and private organizations that interact with the government. There are other industry or sector specific data protection / privacy Acts but those are not covered in this section of the paper. It will be summarized in the relevant sector specific obligations section. The author recommends the reader of this paper to familiarize themselves with the privacy obligations imposed by the individual states. The State Government (except South Australia and Western Australia) and Territories Privacy Acts are:

- Privacy and Data Protection Act 2014 – Victoria
- Personal Information Protection Act 1998 – New South Wales
- Privacy and Information Privacy Act 2009 – Queensland
- Personal Information Protection Act 2004 – Tasmania
- Information Privacy Act 2014 – Australian Capital Territory
- Information Act 2002 – Northern Territory

In Australia, most state governments tend to follow federal government Acts (also known as Commonwealth Acts). To ensure that there is adequate coverage of both federal and state laws, readers are advised to compare both laws and comply with the one that is broader in scope and restrictive in detail than the other.

3.2. Cybercrime Act 2001

This legislation was enacted due to some of the popular viruses of late 1990s. The Australian Government hoped that this Act will act as a deterrent of cybercrimes that was increasing at a rapid pace (Boulton, 2004). Various industry analysts saw this as a knee-jerk reaction to the highly publicized virus attacks such as "Melissa", "I LOVE YOU" and "Code Red" (EFA, 2015). According to this law the definition of a "computer" is not only a desktop or laptop computer, but also a tablet or smartphone. Similarly the definition of a "network" is broader than the Internet; it includes a corporate intranet and even the various devices at an individual's home connected either by cables or by Wi-Fi network. Individuals and organizations must be careful and understand how this law could be interpreted in the event a perpetrator uses the organization's computer or network for committing crime (i.e., computer or network acts as a carrier).

This law was amended on 1 March 2013 and establishes the legislative framework for Australia's accession to the Council of Europe Convention on Cybercrime. This law has close relation with a number of other existing Commonwealth statutes, including the *Mutual Assistance in Criminal Matters Act* 1987 (Cth), the *Crimes Act* 1914 (Cth), the *Criminal Code Act* 1995 (Cth), the *Telecommunications (Interception and Access) Act* 1979 (Cth) and the *Telecommunications Act 1997* (Cth).

The offences covered (implemented in the *Cybercrime Bill* as s.477.1 to 478.4 of the *Criminal Code Act*) (EFA, 2015) are:

- Unauthorised access, modification or impairment to commit a serious offence
- Unauthorised modification of data to cause impairment
- Unauthorised impairment of electronic communications
- Possession of data with intent to commit computer offence
- Supply of data with intent to commit a computer offence
- Unauthorised access to restricted data
- Unauthorised impairment of data held in a computer disk, credit card, and so forth

The cybersecurity related offenses are addressed in the Criminal Code Act 1995 (Criminal Code). These offences are based on model laws agreed to by Commonwealth, state and territory governments in 2001. According to the Attorney General's website, "the offences are consistent with those required by the Council of Europe Convention on Cybercrime and are drafted in technology-neutral terms to accommodate advances in technology" (AG, 2015). Criminal code Act 1995 and Crimes Act 1914 will not be discussed any further in this document. The author urges the readers to consult with their legal team for any specific advice.

3.3. Spam Act 2003

Spam Act 2003 is enforced by Australian Communications and Media Authority (ACMA). Australian businesses that fail to comply with this act can be fined up to AUD $1.1 million per day for repeat corporate offenders (BIT, 2015). This Act prohibits the sending of unsolicited commercial electronic messages via email, Short Message Service (SMS), Multimedia Message Service (MMS) and instant messages with an Australian link. If the spam originates in Australia or a spam is destined to a recipient in Australia, it is said to have an Australian link. Voice calls and fax messages are not covered by this Act; instead these two are managed by "do not call register" maintained by ACMA. Government bodies, registered charities, political parties, and educational institutions can send messages without consent. All others have to comply with three main rules – ***Consent*** - only send commercial electronic messages with the addressee's consent either express or inferred, ***Identification*** - include clear and accurate information about the person or business that is responsible for sending the commercial electronic message and ***Unsubscribe*** - ensure that a functional unsubscribe facility is included in all commercial electronic messages and deal with unsubscribe requests promptly.

The full definition of a commercial message according to ACMA (ACMA1, 2015) is one that:

- Offers, advertises or promotes the supply of goods, services, land or business or investment opportunities.
- Advertises or promotes a supplier of goods, services, land or a provider of business or investment opportunities.

- Helps a person dishonestly obtain property, commercial advantage or other gain from another person.

There are two types of consent, express consent and inferred consent. Express consent means the message receiver has deliberately and intentionally opted-in to receive electronic messages from the sender. Examples of express consent include: voluntarily providing email address; ticking a box next to a consent acceptance page on a website; providing a mobile number to receive such messages. Inferred consent assumes that there is already an established relationship with the message sender. This type of consent is tricky and the message sending organization must tread carefully before sending commercial messages. For example, if an individual already has a relationship with a bank as a bank's customer, this bank is not allowed to use the current relationship to send unsolicited commercial emails pertaining to their other offerings unless the bank has express consent from the customer.

All commercial electronic messages must have clear and accurate identification information so that the receiver can contact the sender. Identifying information can be the 'from' field or subject line of an email, a website address, identification of an SMS or MMS message and the body of the message text.

Sender's commercial messages must have an un-subscribe facility with clear instructions on how to un-subscribe. Some un-subscribe facility can be a text message reply 'Stop' to un-subscribe, preference change option on a website or an un-subscribe link at the bottom of commercial electronic message.

3.4. Telecommunications (Interception & Access) Act 1979

This Act applies to all Internet Service Providers (ISP) and Telecommunications Network providers. The main purpose of this Act is to make it an offence for a person to intercept or access private telecommunications without the knowledge of those involved in that communication. Such persons could be any common citizen or an unauthorized employee of the service providers. Authorized employees of a service provider can have access to such information to perform their day to day duties (Fair, 2013).Access to such communications is also allowed for law enforcement and national security purposes. Various agencies (government and law enforcement) can access communications either

in real time or stored communications (such as emails, SMS messages or recorded voice calls) for their investigations after obtaining a warrant from a court or tribunal. A recent amendment to this Act (enacted on 13 April 2015) also permits Australian agencies to access telecommunications data. This metadata is the information associated with a communication, such as telephone call records or account holder names, website access details, geolocation details of a mobile phone, access time and duration (AG2, 2015).

According to the information published on the Australian Government's website (AG3, 2015), the primary reason for taking this step lies in the fact that "metadata plays a central role in almost all serious criminal and national security investigations," which is why law enforcement and security agencies need to be able to "lawfully access this kind of data in connection with their investigations." But many media outlets and citizens of Australia consider such access is very intrusive impacting the privacy of ordinary Australian citizens. ISPs and telecommunications providers must familiarize with the new amendment to this Act and implement recommendations by October 2015. Because of this amendment, ISPs and telecommunication providers should also pay attention to the new Australian Privacy Principles since access and processing metadata comes under purview of the Privacy Act 1988.

3.5. Other Federal legislative Acts

The federal Acts discussed in sections 3.1 to 3.4 commonly applies to most governmental and private organizations in Australia. Other federal Acts either complement the discussed Acts or form the basis of those Acts. Table 2 highlights (DPC-SA, 2015) (Protectivesecurity, 2015) those Acts that are important from a cybersecurity perspective. Readers of this paper should either be familiar with these Acts or obtain guidance from their legal team. These Acts can be accessed at https://www.comlaw.gov.au/.

Table 2 – Other Applicable Legislative Acts

Reference Act	Cybersecurity Relevance
Australian Security Intelligence Organisation	Establishes and prescribes ASIO's functions and powers. Includes provisions for computer access warrants, security

Reference Act	Cybersecurity Relevance
(ASIO) Act 1979	assessments, and listening and tracking devices.
Crimes Act 1914	Codifies offences against the Commonwealth. Functions alongside State legislation and is gradually superseding the Criminal Code Act 1995.
Criminal Code Act 1995	The main piece of legislation containing federal offences. Abolishes all common law offences and is gradually superseding the Crimes Act 1914.
Electronic Transactions Act 1999	Provides a regulatory framework that recognises the importance of the information economy and facilitates the use of electronic transactions.
Intelligence Services Act 2001	Provides parliamentary and judicial support for the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD). Also grants powers to Australian Security Intelligence Organisation (ASIO).
National Security Information (Criminal and Civil Proceedings) Act 2004 (Cth)	Prevents the disclosure of information in federal criminal and civil proceedings where the disclosure is likely to prejudice national security, except where preventing the disclosure would seriously interfere with the administration of justice.

4. Voluntary Code of Conduct (Guidelines)

A voluntary code of conduct aims to help industry members improve business practices and meet their regulatory obligations. It sets out specific standards of conduct – voluntarily agreed to by signatories about how industry members deal with each other and their customers. An effective industry code can provide greater protection for consumers and reduce the regulatory burden for business (ACCC, 2011). Voluntary guidelines are either industry agreed or an organizations willingness to adopt a pre-defined best practice to improve its business as usual (BAU) operations. From

cybersecurity perspective, such guidelines improve cybersecurity posture of the adopting organization and minimize risks from either deliberate or accidental threat actors.

Although Australia lacks specific cybersecurity regulations like HIPAA (Health Insurance Portability and Accountability Act), NERC-CIP, GLBA Act (Gramm-Leach-Bliley) and so forth, many industry verticals are proactive in either agreeing to a common voluntary cybersecurity guideline or to adopt frameworks published by other countries. One such example is NIST Cybersecurity Framework for Critical Infrastructure, recommended by the Australian Securities and Investment Corporation (ASIC). This section highlights some of the voluntary guidelines proposed by various industry groups that can be adopted by many organizations. Where such voluntary guidelines are nonexistent, the author has recommended few from other countries. One of the advantages of adopting such guidelines is the minimal gap to compliance with a specific legislation or a regulation when it is enacted in the future.

4.1. Guidelines for Utilities

There are no specific regulations or guidance for utilities in Australia. Over many years most of the good cybersecurity guidance and information sharing has happened through the Attorney General's Trusted Information Sharing Network's (TISN) SCADA Community of Interest (CoI) group. TISN has published a few guidelines but only two document for SCADA named "SCADA: Generic Risk Management Framework" (TISN, 2015) and "SCADA: Advice for CEOs". Lack of good guidelines is documented by Christopher Beggs in his paper titled "A Holistic SCADA Security Standard for the Australian Context" (Beggs, 2008).

Some non-Australian cybersecurity guidelines and frameworks that could help Australian utilities are listed below. Prior to adoption, readers are encouraged to assess the suitability, cost and time to.

- NERC Critical Infrastructure Protection (CIP), Reliability Standard version 7: This standard is applicable to electricity utilities and is available at http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

- ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls and available at http://www.iso.org/iso/catalogue_detail?csnumber=54533
- ISO/IEC TR 27019:2013 Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry and is available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security and is available at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

4.2. Guidelines for Mining industry

There are no specific regulations or guidance for mining industry in Australia. Due to the lucrative nature of the business, in recent years mining industry is a target of corporate espionage, extortion and information stealing (Burrell, 2015). Since most of the mining organizations also have Industrial Control Systems (ICS), it is prudent to consider the resources listed in Section 4.1.

4.3. Guidelines for Manufacturing Industry

There are no specific regulations or guidance for manufacturing industry in Australia. As a starting point, manufacturing industry should consider using ISO/IEC 27002:2013 as their security framework. For organizations that have ICS systems, such as for chemical and pharmaceutical manufacturing, they can consider adopting NIST SP 800-82 guidelines.

4.4. Guidelines for Federal Government Agencies

The federal government has mandated that all federal agencies comply with the Protective Security Policy Framework (PSPF) and the associated Information Security Manual ISM). PSPF and ISM form a comprehensive framework that provides the appropriate controls for the Australian Government to protect its people, information and

assets, both at home and overseas. ISM was developed by the Australian Defense, Australian Signals Directorate (ASD) and is the standard which governs the security of government Information and Communication Technology (ICT) systems. Both PSPF and ISM requirements must be met by the organizations (supply chain) that provide services to federal government. InfoSec Registered Assessors Program (iRAP) assessors provide cyber security assessment services to Australian governments. Guidelines for State Government Agencies

Most of the states have their own Information Security Management Frameworks (ISMFs). Although not mandatory, many state governments are adopting the PSPF- ISM framework. It is prudent for these agencies to follow PSPF-ISM since they interact with Federal Government agencies using IT systems. To reduce duplication efforts, it is recommended to perform a gap assessment of the individual state ISMFs with PSPF-ISM and focus compliance efforts only on those gaps.

4.5. Guidelines for Banking, Finance, Insurance and Superannuation Industry

Two regulatory bodies, Australian Prudential Regulatory Authority (APRA) and Australian Securities and Investment Corporation (ASIC) provide some guidance in relation to cybersecurity guidelines. Some of the banks who operate in other countries already must comply with regulations local to those countries such as GLBA, BASEL II and the like. One important recent development by ASIC is the publication of "Report 429: Cyber Resilience – Health Check". This guideline was released in March 2015 and focuses on key questions Board of Directors must ask to ensure good cyber resilience practice is in place. This report is based on the "NIST Cyber Security Framework for Critical Infrastructure". Although at this stage it is just a guideline, there are discussions that this could be mandated by ASIC to all Australian Stock Exchange (ASX) listed organizations.

Other important documents providing guidance from APRA and ASIC are briefly described below.

- "Prudential Practice Guide CPG 235- Managing Data Risk", provides information about data risk governance and management. This guideline

can be accessed at http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk.pdf

- "Prudential Practice Guide PPG 234- Management of security risk in information and information technology", provides guidance on user awareness, access controls, IT asset management, monitoring, security reporting, security assurance and security incident management. As additional attachments, this document provides further guidance on change management, secure software development, cryptographic controls and customer protection. This guideline can be accessed at http://www.apra.gov.au/crossindustry/documents/ppg_ppg234_msrit_012010_v7.pdf
- ASIC's Australian Financial Services License (AFSL) holders must comply with sub sections Regulatory Guide RG 104.93 and RG 104.96 of section RG 104. These sections highlights licence obligations in relation to human resource security, maintaining client record security and IT systems security. This guideline can be accessed at http://download.asic.gov.au/media/1240097/rg104.pdf
- ASIC Report 429: This report is game changing as it is a clear message from ASIC around best practice and governance requirements when it comes to cyber resilience. The report clearly highlights the responsibility of the Board of Directors and senior management in being aware, and having oversight of cyber risks, particularly the duties placed on directors under the Corporations Act. Report 429 is largely based on the "NIST Cyber Security Framework for Critical Infrastructure" document. Cyber Resilience – Health Check can be accessed from http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.

4.6. Guidelines for Internet Service Providers and Telecommunication Providers

ISPs have no other Acts or regulatory requirements apart from the recently enacted data retention bill (Telecommunications (interception & Access) Amendment (Data Retention) Act 1979). The Communications Alliance was formed to provide a unified voice for the Australian communications industry, offering a forum for the industry to make coherent and constructive contributions to policy development and debate (Commsalliance 1, 2015). The Alliance took over the responsibility for the Industry Codes (iCodes) and core responsibilities of the Internet Industry Association (IIA) under an agreement signed on 24 March 2014. C650:2014 iCode is a voluntary code adopted by all ISPs in Australia. The iCode aims to (Commsalliance, 2014):

- Instil cyber-security culture within Australian ISPs and their customers;
- Provide consistent messaging and plain language information to customers;
- Encourage ISPs to identify compromised devices on their networks;
- Encourage ISPs to identify, communicate with each other and report any cyber security issue that may affect Australia's critical infrastructure, or may have a national security dimension; and
- Implement these measures in a manner that protects the privacy of customers, consistent with relevant legislative obligations.

Another voluntary initiative promoted by the ISPs under Australian Communications and Media Authority (ACMA) stewardship is Australian Internet Security Initiative (AISI). This initiative help address the problem of compromised computers (sometimes referred to as 'zombies', 'bots', or 'drones').

4.7. Guidelines for Health Care Providers

Sections 135AA, 135 AB and 135AC of National Health Act 1953 specifically address privacy rules, breach of privacy rules and authorization of collection of health information respectively. These sections very clearly explain the obligations under the Privacy Act 1988, but, apart from this Act, there are no other regulatory obligations in relation to cybersecurity. The Royal Australian College of General Practitioners

(RACGP) has released three guidance documents to help health care providers to implement appropriate cybersecurity controls to safeguard patient data and secure IT systems.

The first document "Computer and information security standards for general practices" consists of twelve domains. In each domain there are specific actions and controls aligned in line with five levels of compliance maturity indicators (initial, repeatable, defined, managed and optimised). Depending on the critical domain, the minimum compliance requirements is either Level 3-defined or Level 4-managed.

The second document is "Standards for general practice - fourth edition" and in section four – Practice Management, standard 4.2 "Management of health information" provides guidance on information security and confidentiality & privacy of health information.

The third document "Compliance indicators for the Australian Privacy Principles" specifically addresses the indicators of compliance with the Australian Privacy Principles. These documents can be accessed at,

- http://www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/
- http://www.racgp.org.au/your-practice/standards/standards4thedition/
- http://www.racgp.org.au/download/Documents/Standards/CIS-APPcompliance.pdf

5. Conclusion

There is no escape for private organizations and government agencies in Australia from complying with regulatory obligations. Non-compliance is expensive and security managers must be on top of changing regulatory environment in their domains. In today's world of ever increasing data breaches, identity thefts, state sponsored cybersecurity intrusions and privacy disclosures; it is more than prudent to comply with regulatory obligations.

Babu Veerappa Srinivas, babuseenu@gmail.com

Despite debates highlighting the pros and cons and the effectiveness of regulation in an era of constant technological change, the author believes that compliance with these obligations and adoption of voluntary cybersecurity codes and standards should be seen as business enablers. Good cybersecurity practices can improve stakeholder confidence, minimises system downtimes and potentially provide other ancillary benefits (*Good Cyber is Good Business*, 2013).

It is also important to note that there is no one size fit all framework. It is advisable to adopt two or three leading frameworks such as NIST Cybersecurity Framework for Critical Infrastructure, Australian Privacy Principles and Australian Government PSPF and ISM to get better coverage of controls. Organizations that comply with such combination of two or more frameworks may be better positioned to comply with future cybersecurity and privacy regulations (*Why you should adopt the NIST Cybersecurity Framework*, 2014).

Security managers and practitioners are encouraged to research regulatory framework and voluntary standards that are available for their industry. This will help others in the industry to know more about these standards and potentially adopt those standards. Increased adoption of such frameworks will lift the security baseline in a particular industry. This is an iterative process and research in exploring such frameworks should continue incessantly.

Since the cyber threats are evolving rapidly (Verizon, 2015) and are affecting every industry and government sector, the regulatory or the governing bodies are investing time and efforts in publishing latest guidance related to cyber security. Readers are encouraged to research specific guidance and obligations imposed by their relevant governing authority for the latest information. They should also keep an eye on the future changes in every Act and Regulation pertaining to cybersecurity and strive to comply with those requirements for the benefit of both of their organization and their community.

Babu Veerappa Srinivas, babuseenu@gmail.com

6. References

ACCC. (2011). *Guidelines for developing effective* (p. 1). Sydney: ACCC. Retrieved 14 June 2015, from https://www.accc.gov.au/system/files/Guidelines%20for%20developing%20effective%20voluntary%20industry%20codes%20of%20conduct.pdf

ACMA. (2015). *Australian Internet Security Initiative (AISI) | ACMA*. Retrieved 19 May 2015, from http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative

ACMA1. (2015). *Key elements of the Spam Act | ACMA*. Retrieved 23 May 2015, from http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/key-elements-of-the-spam-act-ensuring-you-dont-spam-i-acma

AG. (2015). *Cybercrime | Attorney-General's Department*. Retrieved 22 May 2015, from https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx

AG2. (2015). *Overview of legislation | Attorney-General's Department*. Retrieved 23 May 2015, from https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Overviewoflegislation.aspx

AG3. (2015). *Frequently asked questions | Attorney-General's Department*. Retrieved 23 May 2015, from https://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Frequentlyaskedquestions.aspx

Asic.gov.au. (2015). *15-060MR ASIC issues major cyber resilience report | ASIC - Australian Securities and Investments Commission*. Retrieved 18 May 2015, from http://asic.gov.au/about-asic/media-centre/find-a-media-release/2015-releases/15-060mr-asic-issues-major-cyber-resilience-report/

Beggs, C. (2008). *A Holistic SCADA Security Standard for the* (1st ed., pp. 7-10). Melbourne: Sinclair Knight Merz Pty Ltd. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1024&context=isw

BIT. (2015). *Don't get stung by Australia's anti-spam laws*. Retrieved 22 May 2015, from http://www.bit.com.au/News/316120,dont-get-stung-by-australias-anti-spam-laws.aspx

Boulton, A. (2004). *Synopsis of the Cybercrime Act 2001*. *Giac.org*. Retrieved 14 June 2015, from http://www.giac.org/paper/gsec/4017/synopsis-cybercrime-act-2001/106427

Burrell, A. (2015). *Miners under cyber attack 'from everywhere'*. *The Australian Business Review*. Retrieved 31 May 2015, from http://www.theaustralian.com.au/business/mining-energy/miners-under-cyber-attack-from-everywhere/story-e6frg9df-1226065199596

Cisco,. (2015). *Design Zone for Security*. Retrieved 15 May 2015, from http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html?

CISecurity, T. (2015). *Center for Internet Security :: Security Benchmarks Division :: CIS Download Form*. *Benchmarks.cisecurity.org*. Retrieved 15 May 2015, from https://benchmarks.cisecurity.org/downloads/multiform/index.cfm

Commsalliance,. (2014). *Communications Alliance - Internet Service Provider Industry*. Retrieved 2 June 2015, from http://www.commsalliance.com.au/Activities/ispi

Commsalliance 1,. (2015). *Communications Alliance - Overview*. Retrieved 14 June 2015, from http://www.commsalliance.com.au/about-us/overview

CSRC. (2015). *NIST Computer Security Publications - NIST Special Publications (SPs)*. Retrieved 15 May 2015, from http://csrc.nist.gov/publications/PubsSPs.html

Cybersecurity policy making at a turning point. (2012) (2nd ed., p. 11). Retrieved from http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Cyber-security risks in the supply chain. (2015) (1st ed., pp. 3-6). London. Retrieved from https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf

DPC-SA. (2015). *Policies, Standards and Guidelines*. Retrieved 24 May 2015, from http://dpc.sa.gov.au/sites/default/files/pubimages/documents/ocio/ISMFguideline38%28legislation%29.pdf

EFA. (2015). *Cybercrime / Computer Crime Legislation*. Retrieved 22 May 2015, from https://www.efa.org.au/Issues/Privacy/cybercrimeact.html

Fair, P. (2013). *Cyber Security - Overview of the Regulatory Environment* (1st ed., p. 10). Sydney: Baker & McKenzie. Retrieved from http://www.commsalliance.com.au/__data/assets/pdf_file/0016/40147/B-and-M-CommsAlliance-Cyber-Security-Presentation-30May13.pdf

Germano, J., & Goldman, Z. (2014). *After the breach: Cybersecurity liability risk* (1st ed.). New York: New York University School of Law. Retrieved from http://www.lawandsecurity.org/Portals/0/Documents/CLS%20After%20the%20Breach%20Final.pdf

Good Cyber is Good Business. (2013) (1st ed., p. 13). London. Retrieved from https://www.thalesgroup.com/sites/default/files/asset/document/cyber-security-audit-test-and-compliance.pdf

Greenwald, J. (2015). *Sony hack spurs bipartisan support of cyber security legislation - Business Insurance*. *Business Insurance*. Retrieved 18 May 2015, from http://www.businessinsurance.com/article/20150201/NEWS06/150139967

IBM. (2015). *IBM Redbooks | Security*. Retrieved 13 May 2015, from http://www.redbooks.ibm.com/portals/security

Iso.org. (2015). *ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls*. Retrieved 16 May 2015, from http://www.iso.org/iso/catalogue_detail?csnumber=54533

Microsoft,. (2015). *Security for IT Pros*. Retrieved 16 May 2015, from https://technet.microsoft.com/en-au/security/

Oracle. (2015). *Security Topic: Articles & Whitepapers*. Retrieved 17 May 2015, from http://www.oracle.com/technetwork/topics/security/articles/index.html

PCI,. (2015). *Official Source of PCI DSS Data Security Standards Documents and Payment Card Compliance Guidelines*. Retrieved 16 May 2015, from https://www.pcisecuritystandards.org/security_standards/

Protectivesecurity. (2015). *Legislation*. Retrieved 25 May 2015, from http://www.protectivesecurity.gov.au/governance/Pages/Legislation.aspx

TISN. (2015). *TISN Publications-by-topic*. Retrieved 29 May 2015, from http://www.tisn.gov.au/Pages/Publications-by-topic.aspx

Verizon. (2015). *2015 Data Breach Investigations Report (DBIR)*. Retrieved 5 June 2015, from http://www.verizonenterprise.com/DBIR/2015/

Why you should adopt the NIST Cybersecurity Framework. (2014) (1st ed., p. 5). USA. Retrieved from http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

Wilkerson, T. (2014). *Cybersecurity in the supply chain* (1st ed.). Baltimore: United States Cybersecurity Magazine. Retrieved from http://www.lmi.org/en/News-Publications/News/News-Item?id=208

Wisseman, S. (2015). *Balancing Value, Costs, and Risk for an Effective Security Program*. *Enterprise CIO Forum*. Retrieved 16 May 2015, from http://www.enterprisecioforum.com/en/blogs/hp-security-strategists/balancing-value-costs-and-risk-effective

7. Appendix: Sources for Australia Privacy and Cybersecurity Laws

This appendix provides a reference for the reader who may want to do additional research on the state of privacy and cybersecurity in Australia.

Changes to legal, regulatory and legislative framework can be accessed at:

- https://www.comlaw.gov.au/ for Federal government database
- http://www.legislation.vic.gov.au/ and choose Victorian Law Today for the state of Victoria
- http://www.legislation.nsw.gov.au/ for the state of New South Wales
- http://www.legislation.sa.gov.au/index.aspx for the state of South Australia
- https://www.slp.wa.gov.au/legislation/statutes.nsf/default.html for the state of Western Australia
- https://www.legislation.qld.gov.au/OQPChome.htm for the state of Queensland
- http://www.thelaw.tas.gov.au/index.w3p for the state of Tasmania
- http://www.austlii.edu.au/ general legal database to search cases, laws and legislation

The Privacy Act 1988 (Cth) and the privacy principles can be accessed at:

- Privacy Act: http://www.comlaw.gov.au/Details/C2015C00089
- Privacy Principles: http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles
- Privacy fact sheets – applicable to relevant industry: http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/

Additional artefacts to alleviate confusion and to assist organizations in complying with this Act were released by the OAIC. They are,

- A revised and updated guide to securing personal information was issued in January 2015: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information
- Updated Australian Privacy Principle (APP) guidelines on 1 April 2015 http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/
- A revised an updated data breach notification guide was issued in August 2014: http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/data-breach-notification-guide-august-2014.pdf
- A privacy management framework – provides steps the OAIC expects organisations to take to meet their ongoing compliance obligations under APP 1.2: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-management-framework
- Results of its assessment of the online privacy policies of 20 Australian and international organisations from the finance, online retail, government, social and other media sectors. http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-policies-still-have-room-for-improvement
- Handling privacy complaints resource – is intended to help organisations and agencies covered by the Privacy Act address privacy complaints they receive: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/handling-privacy-complaints

The Cybercrime Act 2001 and the associated amendments can be accessed at,

- http://www.comlaw.gov.au/Details/C2004A00937 - Cybercrime Act 2001
- http://www.comlaw.gov.au/Details/C2012A00120 - Cybercrime amendment Act 2012

The Spam Act 2003 and the supporting guidance document can be accessed at,

- http://www.comlaw.gov.au/Details/C2014C00214 - Spam Act 2003
- http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/spam-spam-act-2003-faqs - Spam Act FAQs
- http://www.acma.gov.au/Industry/Marketers/Anti-Spam/Ensuring-you-dont-spam/spam-legislation-enforcement-ensuring-you-dont-spam-i-acma - Spam legislation and enforcement

The Telecommunications (Interception & Access) Act 1979 and the supporting guidance document can be accessed at,

- http://www.comlaw.gov.au/Details/C2013C00361 - Telecommunications (interception & Access) Act 1979
- http://www.comlaw.gov.au/Details/C2015A00039 - Telecommunications (interception & Access) Amendment (Data Retention) Act 1979
- https://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Frequentlyaskedquestions.aspx - Data retention FAQ

Other artefacts pertaining to ISPs and telecommunications organizations are,

- The iCode C 650 can be downloaded from http://www.commsalliance.com.au/__data/assets/pdf_file/0019/44632/C650_2014.pdf
- More information on AISI can be accessed at http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative
- Law enforcement and national security obligations of an ISP can be accessed at http://www.acma.gov.au/Industry/Internet/Licensing--I-want-to-be-an-ISP/Carriage-service-provider-rules/isps-and-law-enforcement-isp-licensing-i-acma

Federal Government (Commonwealth Government) Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) artefacts can be accessed at,

- http://www.protectivesecurity.gov.au/Pages/default.aspx
- http://www.asd.gov.au/infosec/ism/

Individual State Government information security resources can be found at,

- Victoria - http://www.digital.vic.gov.au/resources/information-security/
- South Australia - http://dpc.sa.gov.au/policies-standards-and-guidelines#Security
- New South Wales - http://arp.nsw.gov.au/m2012-15-digital-information-security-policy
- Queensland - https://www.qgcio.qld.gov.au/products/information-security/information-security-toolbox
- Tasmania - http://www.egovernment.tas.gov.au/standards_and_guidelines/tasmanian_government_information_security_framework and http://www.egovernment.tas.gov.au/information_security_and_sharing