MITRE TECHNICAL REPORT

MITRE

Analysis of the NIST Mobile Device Security Practice Guide's Applicability to Australia

Prepared for
AustCyber–the Australian Cyber Security Growth Network

Authors: Christopher Brown
Sallie Edwards
Irving Lachow

March 2018

Approved for Public Release; Distribution Unlimited 18-0982

Executive Summary

The Australian Cyber Security Growth Network (AustCyber) contracted with The MITRE Corporation (MITRE) to assess the applicability of the National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide for *Mobile Device Security: Cloud and Hybrid Builds* (the Practice Guide) to organizations within Australia to consider opportunities for standards harmonization and proactive regulatory reform.

Mobile devices, most frequently in the form of smartphones and tablets, are a key feature of Australia's society and its business activities—securing those devices and the data they carry is critical. While MITRE has considered the role of government and larger enterprises in this report, considerable attention is paid to small and medium-size enterprises (SMEs) due to their important role in the Australian economy. Many of these organizations have limited operational knowledge of cybersecurity. Australian organizations, and particularly SMEs, need practical advice that helps them understand their need for cybersecurity, along with easily consumable guidelines that are affordable and easy to implement.

MITRE found that the abundance of standards and guidelines available to Australian organizations at both the federal and state/territory level caused confusion around what advice should be adopted. "Cyberaware" organizations are overregulating, doing nothing, or applying a mixture of domestic and international standards for guidelines. The result is inefficient and is a barrier to improving Australia's cyber resilience. The Australian government can begin to address this issue by taking steps to harmonize the guidelines it provides to industry and other levels of Australian government.

This report is a starting point for Australian government and industry to further examine the existing overlaps and gaps that Australian organizations face in following the multiple cybersecurity requirements and guidelines. MITRE found that the Practice Guide is helpful to Australian organizations, including government, because it offers comprehensive standards-based guidelines. The Practice Guide attempts to provide practical, real-world security guidelines that most organizations can adopt on unclassified networks. For smaller organizations, the Practice Guide focuses on the use of cloud architecture on mobile devices, while more mature organizations are given guidelines on the use of hybrid architecture.

MITRE identified the Australian Signals Directorate's (ASD) Information Security Manual (ISM) and the Essential Eight mitigation strategies as having the most relevance to mobile device security for organizations in Australia, as well as the Office of the Australian Information Commissioner's (OAIC) guide to securing personal information when considering the recent Privacy Amendment (Notifiable Data Breaches) Act 2017. These three resources were mapped to the Practice Guide to identify overlaps and gaps.

Overall the ISM had the strongest relationship to the Practice Guide, and the gaps identified are largely due to the difference in the intended audience. The Practice Guide was designed for industry, whereas the ISM is focused on defense and federal agencies. The Essential Eight were found to be useful guidelines for mobile device security, with the Practice Guide security characteristics addressing six of the eight Essential Eight strategies. The OAIC guide to securing

personal information is also relevant for SMEs concerned about mobile device security, though it also has broader applicability.

In summary, our analysis showed that the Practice Guide provided useful and practical guidelines on the specific issue of mobile device security within the Australian ecosystem. The Practice Guide can be a useful adjunct to the existing set of Australian guidelines and could serve as a preeminent and comprehensive reference for organizations seeking to improve the cybersecurity of mobile devices. Furthermore, the Practice Guide could become even more useful for SMEs with several modifications described at the conclusion of this report. MITRE recommends that AustCyber, a government-funded and industry-facing independent entity, take the lead in facilitating intergovernmental and multistakeholder discussions on cybersecurity standards harmonization both domestically and internationally (the latter is especially relevant for organizations that export and/or have multinational operations), with mobile device security serving as the initial use case because of its broad applicability across both SMEs and larger enterprises.

Table of Contents

1 Introduction

Australian organizations attempting to secure their cyberenvironment face a complex mix of regulations, standards, and guidance. Businesses that desire to do business with governments face competing standards that are recommended, if not required, by different government agencies. A perceived lack of practical cybersecurity guidance has left some businesses struggling to comply with stringent security controls that exceed the level of security necessary for their environment and often with the levels of security appropriate for implementing their solutions in customer environments.

Further complicating matters is the fact that the Australian economy is driven by small- and medium-size enterprises (SMEs). The criteria defining an SME varies. The Australian Bureau of Statistics (ABS) defines an SME as a business employing 20 people or fewer, while the Australian Tax Office (ATO) defines a small business as an entity with less than AU$10 million in yearly turnover [1] and a large business with turnover of more than AU$250 million. In fact, the Australian government's 2014 Financial System Inquiry report found that Australia's two million small- to mid-size organizations employ almost 70 percent of the total workforce and contribute half of the output of the private sector [2]. It is unrealistic to expect businesses of this size to comply with inconsistent regulations, standards, or guidance that is better suited for large enterprises with dedicated IT staffs; however, the health and security of SMEs impacts not only individual businesses but government and larger corporations as well.

SME owners rely heavily on mobile devices to carry out key business functions. These SMEs need practical advice to help them be aware of cyber risks when interacting with mobile devices and to implement guidance that will prevent, detect, and respond to cybersecurity incidents. There are some high-level cybersecurity best practices available, such as "Keep your business safe from cyberthreats" and the Stay Smart Online website [3][4]. Each of these online government resources provides valuable broad-level cybersecurity information. However, there is a need for practical information for more specific business functions facing SMEs. Mobile devices, most frequently in the form of smartphones and tablets, are a key feature of Australia's society and its business activities—securing those devices and the data they carry is critical, yet it is not clear how SMEs should best address this challenge. Mobile device cybersecurity is further complicated by the impact of increased cloud service usage to store data that is critical to business operations, as highlighted in a report from the Australian Bureau of Statistics [5]. The

During industry consultations, participants noted several resources that provided practical cybersecurity guidance for mobile devices. The Center for Internet Security (CIS), a nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best-practice solutions for cyberdefense, was mentioned as a resource. The CIS produces "benchmark" best-practice security configuration guides on many topics, including mobile devices. Other examples that were mentioned were the United Kingdom's National Cyber Security Centre (NCSC) Cyber Essentials self-help website and the business-focused mobile device security guidance produced by the Australian government's Stay Smart Online website. While these publications are somewhat similar in nature to the NCCoE practice guides, they lack a strong relationship with a common, internationally accepted cybersecurity framework.

activities conducted to develop this report explore a possible option for providing more specific practical cybersecurity advice for Australian SMEs.

1.1 Background

This report leverages the Mobile Device Security Project performed by the National Cybersecurity Center of Excellence (NCCoE) in the United States. The NCCoE is a public-private partnership that creates practical cybersecurity solutions by using a standards-based approach. NCCoE uses currently available commercial technology to produce easily adaptable solutions to address cybersecurity challenges facing industry. Example solutions or reference architectures are documented in a practice guide that contains three parts:

- Volume A–*Executive Summary*, a high-level overview of the project, including summaries of the challenge, solution, and benefits
- Volume B–*Approach, Architecture, and Security Characteristics*, a deep dive into challenge and solution, including approach, architecture, and security mapping to relevant standards
- Volume C–*How-to* guide providing detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

The National Institute of Standards and Technology (NIST) *Cybersecurity Practice Guide for Mobile Device Security: Cloud and Hybrid Builds* (the Practice Guide), also known as NIST Special Publication 1800-4, is among the cybersecurity practice guides produced by the NCCoE. All NCCoE practice guides leverage the United States' NIST-published *Framework for Improving Critical Infrastructure Cybersecurity,* commonly referred to as the Cybersecurity Framework, or CSF. The Cybersecurity Framework was developed via collaboration among government, industry, and academia in response to White House Executive Order 13636 calling for a framework to reduce cybersecurity risks to critical infrastructure. The framework references globally recognized standards for cybersecurity to guide organizations of all sizes and technical sophistication on elements that should be included in a comprehensive cybersecurity program.

The Practice Guide was published in draft format in November 2015 and authored through a collaborative process among MITRE, industry participants, and NCCoE researchers. Since publication, the Practice Guide has received feedback from the public and cybersecurity industry that will be addressed in an update to the Practice Guide. The forthcoming Practice Guide will focus on the current threat landscape and will incorporate mobile-focused cybersecurity technologies that have evolved since the original publication.

A full mapping of the Practice Guide security characteristics to the Cybersecurity Framework and other relevant standards is included in Appendix A.

1.2 Scope

This project's objective is to assess the applicability of the Practice Guide to Australian organizations by determining how the Practice Guide maps to laws, regulations, standards, and guidelines that drive mobile device security practices within Australia. The remainder of the document describes the approach and analysis used in this effort. Furthermore, this report

provides AustCyber with a recommended path forward for improving mobile device security for Australian organizations.

1.3 Report Structure

Section 2, Mobile Device Environment, describes the use and types of mobile devices within Australian organizations. Section 3, Approach, speaks to the process followed to create this report. Section 4, Identified Laws, Standards, and Guidelines, lists the laws, standards, and guidelines reviewed to create this report. Section 5, Laws, Standards, and Guidelines, maps those laws, standards, and guidelines determined to be most relevant to mobile devices to practice guide security characteristics. Section 6, Findings and Recommendations, suggests modifications where practice guide recommendations may be tailored to best address the mobile cybersecurity concerns facing Australian organizations that have limited cybersecurity expertise.

2 Mobile Device Environment

The first step in our analysis was to understand the Australian environment within which mobile devices are used. This section summarizes that environment by looking at the following issues: the way those devices are utilized, the types of mobile devices used by Australian organizations, and the mobile device threat landscape.

2.1 Mobile Device Usage

Mobile devices have become an integral component of day-to-day operations for Australian businesses. Organizations largely use cloud-based email and social media tools in their day-to-day mobile business applications. Google's GSuite and Microsoft's Office365 services are two commonly cited for basic email functionality. This is due to their low cost, ease of use, and functionality–so these tools are often used without considering the business risks and benefits. A 2014 report by the Australian Communications and Media Authority (ACMA) notes that 47 percent of SMEs connected to the internet used some type of cloud computing service [6]. Further, a 2015 report entitled *Report 1–Australians' Digital Lives* asserts that 26 percent of businesses utilize social media for marketing/advertising purposes [7]. Also, organizations are heavily dependent on cloud-based file backup and accounting systems on mobile devices to store personal information, corporate data, and financial, health, and other sensitive records. Organizations across different sectors tend to allow personal devices to access the aforementioned business applications with very little thought given to threat mitigation. Australian organizations, particularly SMEs that are implementing bring-your-own-device (BYOD) policies, may note a gap at the "how to" level due to the lack of a specific BYOD architecture. This was informed by roundtable discussions where the use of BYOD deployment model by Australian organizations, particularly SMEs, was deemed commonplace.

2.2 Mobile Device Types

Similar to the environment in the United States, organizations in Australia tend to use off-the-shelf mobile devices such as Apple iPhones and various Android devices, including the Samsung Galaxy Series, to conduct business. DeviceAtlas, a popular source of device data, appears to bear this out with iPhone and Galaxy devices composing all the top 20 positions of device usage for Australia [8].

Apple iOS was found to be the preferred platform for organizations overall. A few factors play into this, including a perception that iOS is generally more secure. The wide breadth of available Android devices makes enforcement of security policies even more difficult. The ability for manufacturers to take the Android Open Source Project and modify it to their own needs makes the update cycle unpredictable for businesses [9] [10]. Telecom approval for Android updates adds to the delay of operating system security updates. This is a known global issue and is being addressed in Android 8.0 (Oreo) through Project Treble [11]–which makes the upgrade process easier regardless of device manufacturer and carrier. Finally, organizational device owners did not want to lose access to familiar iOS ecosystem components (such as iMessage). This familiarity and user experience appeared to be the most qualitative factor behind purchasing decisions. In contrast, the Android platform was more customizable for those organizations and individuals with the skills to modify the operating system directly.

2.3 Mobile Threat Landscape

The Practice Guide broadly speaks of threats and vulnerabilities that the portable nature of mobile devices presents to an organization. Threats such as mobile malware, stolen devices, and eavesdropping are mapped to technology solutions used within each architecture. The Practice Guide recognizes that vulnerabilities can occur not only within the operating system but also within third-party developer applications and device firmware. The Practice Guide addresses vulnerabilities found in third-party developer applications, whereas operating system and firmware vulnerabilities were deemed out of scope for the Practice Guide.

In the course of this research, MITRE has attempted to ascertain unique threats in the Australian context that would require modifications to the current Practice Guide. We primarily consulted the NIST Mobile Threat Catalogue (MTC), an online resource that describes, identifies, and structures the threats posed to mobile information systems [12]. Each entry in the MTC contains several pieces of information: an identifier, a category, a high-level description, details on its origin, exploit examples, common vulnerabilities and exposures (CVEs) examples, possible countermeasures, and academic references. The threats identified within the MTC align with the threats identified in the ASD's Protection Profile for Mobile Device Fundamentals, which provides security requirements for the evaluation of IT products. Thus, the threat landscape is largely the same as what is experienced in the United States (lost devices, malware, ransomware, etc.) [12].

Additionally, device owners expressed concerns that indicated security is still viewed as an obstacle to usability. This can lead to undesirable behavior where end users attempt to disable security controls to accomplish business tasks. Those organizations aware of the importance of cybersecurity remain concerned about the onerous nature of technical activities necessary to implement mobile device security controls. In particular, SMEs tend to focus on day-to-day business operations and have little time to think about security. One way to address that challenge is to include stories and/or infographics to SMEs that identify risks posed by the use of mobile devices and how mobile device security impacts them.

However, there are a few threats worthy of more investigation, including scams that port phone numbers without device owner consent [13] and phishing attempts designed to trick victims into handing over valuable personal information such as bank account details and passwords [14].

Furthermore, SMEs increasingly need to travel overseas for business and do not often understand that such travel increases the risks around their mobile device. A good reference point for SMEs is guidance provided by smaller government agencies across the tiers of Australian governments on the risks to their staffs, such as the South Australian government's ISMF Guideline 30a on *Working Away from the Office or Abroad*.

Mobile payment methods are an evolving threat vector to monitor in the future, especially for SMEs. External credit card readers such as the Square Reader allow small businesses to accept credit card payments from a consumer mobile device [15]. Modern versions of these peripherals operate using Bluetooth technology, which is vulnerable to a wide range of attacks, especially if not configured properly. Organizations should ensure that any external peripheral follows Bluetooth best security practices, such as those presented in NIST's Special Publication 800-121 Revision 2 *Guide to Bluetooth Security* [16].

3 Approach

MITRE followed a four-step process to assess the applicability of the Practice Guide to Australian organizations:

- Step 1: MITRE collaborated with AustCyber to identify existing mobile device cybersecurity-related laws, regulations, standards, and guidelines that guide the behavior of Australian organizations (Appendix C).
- Step 2: Upon review, MITRE selected from the initial list of more than 40 existing laws, standards, and guidelines to map those identified as most relevant to the guidelines found in the Practice Guide.
- Step 3: MITRE conducted analysis, including holding on-site consultations with Australian organizations. These consultations included stakeholders from the Australian federal and state governments, telecommunications industry, university and research community, industry associations, and SMEs. This research and analysis allowed us to determine if the Practice Guide could be adopted "as is" by Australian organizations and to suggest modifications as appropriate.
- Step 4: Summarized findings and recommendations in the final report. Here we documented the results of our research, comparing security characteristics included in the ISM, Essential Eight, and privacy guidelines, to the Practice Guide. We stated how the Practice Guide aligns with Australian mobile device security standards and guidelines as well as gave recommendations for tailoring it for the needs of Australian organizations.

3.1 Assumptions

This report refers to Australian organizations generally, but it is most applicable to small and medium enterprises. For the purposes of this research, an SME may follow either the Australian Tax Office definition of an entity with less than AU$10 million in yearly turnover, and less than a large business with turnover of more than AU$250 million; or the Australian Bureau of Statistics definition of a business employing fewer than 20 people [17]. Also, this report uses the NIST definition of a mobile device as having the following characteristics [18]:

- a small form factor

- at least one wireless network interface for network access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with connectivity to the internet or other data networks
- local, built-in (nonremovable) data storage
- an operating system that is not a full-fledged desktop or laptop operating system
- applications available through multiple methods (provided with the mobile device, accessed through web browser, acquired and installed from third parties)

This report refers to the cloud and hybrid reference architectures described within the Practice Guide. The cloud architecture is geared toward smaller organizations wanting to operate and maintain systems external to their enterprise environment to lower operational expenses. The hybrid architecture is meant for more mature organizations that are concerned with the risks associated with storing and processing confidential enterprise information in the cloud. Each documented architecture is based on a set of security characteristics that are required to mitigate in large part the risks of storing enterprise data on mobile devices and transmitting enterprise data to and from mobile devices. The identified security characteristics are data protection, data isolation, monitoring, identity and authorization, and privacy [19]. These characteristics are specifically crafted to address the unique mobile security environment rather than general IT security.

For this project, MITRE focused on standards and guidelines most broadly relevant to Australian entities that use mobile devices as tools to conduct business. An exhaustive mapping of all documents that may affect any Australian organization is beyond the scope of this document.

4 Identified Laws, Standards, and Guidelines

In this report, the term “laws” refers to binding rules that are required for applicable entities. Standards establish specifications to ensure reliability and consistency, while guidelines provide optional information or advice [20]. There is some overlap between standards and guidelines. Documents that function as optional guidelines for some entities may be considered standards for another in the sense that they are used to measure compliance to mandates. Deciphering cybersecurity-related laws, standards, and guidelines is a significant challenge for SMEs. It is further complicated by the fact that guidelines produced by government agencies across the federal and state levels are often inconsistent, which could be confusing for industry.

MITRE researched Australian laws, standards, and guidelines to identify those with specific application to mobile device security. General, government, and privacy items that were reviewed are listed in the following table. A description of each regulation or standard and how it does or does not apply to mobile device security is provided in the narrative following the table.

Each of the documents in the following table was deemed to be potentially relevant for mobile device security implementations in Australia. Our analysis describes each law, standard, and guideline and then briefly explains whether it is sufficiently important to be selected for detailed mapping against the Practice Guide.

Table 1—Cybersecurity Laws, Standards, and Guidelines

Name	Type	Issuing Authority	Source
Cyber Security for Contractors	Guidelines (standard for federal government)	Australian Signals Directorate	https://www.asd.gov.au/publications/protect/Cyber_Security_for_Contractors.pdf
Cybercrime Act 2001	Law	Australian Parliament	https://www.legislation.gov.au/Details/C2004C01213
Essential Eight	Guidelines (standard for federal government)	Australian Signals Directorate	https://www.asd.gov.au/publications/protect/essential-eight-explained.htm
ISO 27001/2	Standard	International Organization for Standardization	https://www.iso.org/isoiec-27001-information-security.html
Framework for Improving Critical Infrastructure Cybersecurity	Guidelines	NIST	https://www.nist.gov/cyberframework
Risk Management of Enterprise Mobility, Including Bring Your Own Device	Guidelines	Australian Signals Directorate	https://www.asd.gov.au/publications/protect/enterprise_mobility_bring_your_own_device_byod.htm
Strategies to Mitigate Cyber Security Incidents	Guidelines	Australian Signals Directorate	https://www.asd.gov.au/infosec/mitigationstrategies.htm
Information Security Manual (ISM)	Standard for federal government	Australian Signals Directorate	https://www.asd.gov.au/infosec/ism/
Information Security Management Guidelines: Risk management of outsourced ICT arrangements (including Cloud)	Standard for federal government	Australian Government	https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentInformationSecurityManagementGuidelines.pdf
Information Security Registered Assessors Program (IRAP)	Standard	Australian Signals Directorate	https://www.asd.gov.au/publications/irap/IRAP_Policy_and_Procedures.pdf
Protective Security Policy Framework	Guidelines	Australia	https://www.protectivesecurity.gov.au/Pages/default.aspx
Privacy Amendment (Notifiable Data Breaches) Act 2017	Law	Australian Parliament	https://www.legislation.gov.au/Details/C2017A00012

Privacy Act 1988	Law	Australian Parliament	https://www.oaic.gov.au/privacy-law/privacy-act
Guide to securing personal information	Guidelines	Office of the Australian Information Commissioner	https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

4.1 National Laws

The items listed here are federal laws and were reviewed for their potential applicability to mobile device security in Australia.

4.1.1 Cybercrime Act 2001

The Cybercrime Act 2001 is a law that provides a mechanism to prosecute those who use cyberspace to perpetrate crime. It defines computer offenses, addresses enforcement authority, and outlines penalties for violations. While the act is of interest, it is not directly relevant to improving mobile device security as the emphasis is on hacking and computer crimes; thus, it is not included as a mapping component.

4.1.2 Privacy

While the Commonwealth Privacy Act 1988 (the Privacy Act) and Privacy Amendment (Notifiable Data Breaches) Act 2017 are listed individually in Table 1, they are addressed together here under the Privacy header.

The Privacy Act defines personal information and regulates how it may be handled. The Privacy Act established the 13 Australian Privacy Principles (APP). It intersects with mobile devices due to the myriad of transaction types and tasks conducted via mobile device, some of those actions using personal information. However, it is the Privacy Amendment (Notifiable Data Breaches) Act 2017 that is most noted when addressing mobile device security due to the potential for data breach via a mobile device. The Privacy Amendment (Notifiable Data Breaches) Act 2017 established a mandatory data breach notification scheme in Australia. The amendment is applicable to entities covered in the Privacy Act, including businesses that have an annual turnover of more than AU$3 million, organizations that have Privacy Act security obligations in relation to particular types of information, and other organizations that have voluntarily opted in to Privacy Act compliance [21].

MITRE found that elements of the *Guide to Securing Personal Information* more closely align to mobile device security and selected that document for mapping privacy elements rather than either the Privacy Act or Privacy Amendment (Notifiable Data Breaches) Act 2017.

4.2 Standards and Guidelines

Most of the material published to influence organizations' cybersecurity activity fits within the category of standards and guidelines. Although compliance with standards may be required for certain entities (e.g., federal agencies may have to comply with certain government-mandated standards), standards are typically not treated as mandates by private-sector entities. Guidelines-

level documents are advisory; they provide recommendations and/or suggestions but are purely optional. Although the terms "standards" and "guidelines" appear to be well-defined and distinctive, there is crossover, often due to procurement processes requiring applicants to demonstrate compliance with one or more standards, which creates a confusing area for organizations. From its consultations with industry, MITRE learned that this contributed to some organizations not taking any actions while larger organizations described using a combination of standards and guidelines documents from international and Australian sources, including the NIST Cybersecurity Framework.

This section provides a description of the standards and guidelines documents we deemed to be relevant to the Practice Guide. The focus below is on federal-level documents. However, as part of our research we reviewed the procurement policies of each Australian state and territory. While states do have cybersecurity requirements in their procurement policies, these policies apply only to those organizations that are doing business with the states. This could lead to situations where businesses trying to work with multiple states, as well as with the federal government, are forced to comply with a myriad of different policies. In addition, only the New South Wales state government provided clear guidelines for entities pursuing mobile device procurement through the NSW Government Device & Application Framework. However, the NSW Framework lacks a clear linkage to federal government policies. Organizations doing business with the multiple Australian jurisdictions need to review the procurement policy for each state. This has the potential to further fragment any cybersecurity advice. The list of state procurement policies reviewed for this effort is shown in Appendix D.

4.2.1 Strategies to Mitigate Cyber Security Incidents

ASD's *Strategies to Mitigate Cyber Security Incidents* provides relevant guidelines to all organizations seeking methods to reduce cybersecurity incidents. Along with its companion document *Strategies to Mitigate Cyber Security Incidents–Mitigation Details*, this ASD guideline is a useful resource for Australian organizations. However, these publications focus on enterprise security rather than mobile device security and already incorporate a portion of the Essential Eight [22]; therefore, they are not included in the mapping of the Practice Guide.

4.2.2 Cyber Security for Contractors

ASD's *Cyber Security for Contractors* publication is designed to assist government contractors as they seek to protect government data contained on their systems. The key provisions of the document are the Essential Eight [22]. Because this report has included the Essential Eight in the mapping of the Practice Guide, the inclusion of *Cyber Security for Contractors* publication would be repetitive. Further, the publication recommends that contractors review the guidelines published by the Australian Cyber Security Centre (ACSC). While the ACSC's guidelines are not specifically related to mobile devices, the reader concerned with mobile device security should review *Cloud Computing Security for Tenants,* which lists essential mitigations for data compromise [23]. As discussed earlier in this report, mobile devices often leverage cloud services during business operations.

4.2.3 Essential Eight

ASD's Essential Eight as documented in the *Essential Eight Explained* build on ASD's previous *Top 4 Mitigation Strategies for Targeted Cyber Intrusions* with the goal of being a cybersecurity baseline for organizations [22]. The research undertaken for this project found the Essential Eight to be widely used in Australia, even beyond government organizations, and that they also have some applicability to mobile devices. Therefore, we use the Essential Eight as a basis for mapping to the guidelines found in the Practice Guide.

4.2.4 ISO 27001/27002

The International Organization of Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series of standards is applicable to any entity implementing a mobile device security solution. The Practice Guide includes ISO/IEC 27002, which provides best-practice recommendations on implementing security in its security characteristics mapping. ISO 27002 is included in the currently published version of the Practice Guide; therefore, it is not addressed separately in this document. Those seeking information on how ISO 27002 relates to a mobile device security implementation should review the Practice Guide.

4.2.5 NIST Cybersecurity Framework

Published in February 2014 by NIST, the Cybersecurity Framework is a guide for entities seeking to employ a flexible, risk-based, and comprehensive cybersecurity program. The framework itself is not a standard; rather, it is an approach developed in consensus with industry that is based on standards. The core of the framework includes five functions: identify, protect, detect, respond, and recover. The functions are broken down further into subcategories and cross-referenced with other commonly used standards. The framework provides the basis for the Practice Guide. The full mapping of the Practice Guide to the Cybersecurity Framework can be found in Appendix A.

4.2.6 Risk Management of Enterprise Mobility Including Bring Your Own Device

The *Risk Management of Enterprise Mobility Including Bring Your Own Device* published by ASD provides relevant information for organizations considering deploying a bring your own device (BYOD) policy. It explores risk tolerance and business usage; however, it is not included in our mapping because its focus is on business cases rather than practical implementation guidelines.

4.2.7 Protective Security Policy Framework (PSPF)

The *Protective Security Policy Framework*, authored by Australia's Attorney-General's Department, takes a broad approach to security that includes governance, personnel security, information security, and physical security. Australian government agencies are required to comply with its 36 requirements, and it is provided to state and territory governments as a holistic model for public-sector security management. Because it is a high-level document without a direct correlation to the technical recommendations in the Practice Guide and it applies to the Australian government, it is not included in the mapping provided in the next section.

4.2.8 Information Security Manual

The ISM, authored by ASD, is the flagship document for the application of risk-based information security principles and controls for Australian government agencies, thereby functioning as the standard that governs the security of Australian government information and communication technology (ICT) systems. [24]. The ISM's suggested audience is "Information Technology Security Advisors, Information Technology Security Managers, Information Security Registered Assessors and other security practitioners across government." The role and technical skill level of this audience is similar to the Practice Guide's target audience in its Part B, which is focused on chief information officers, chief information security officers, and security managers. While the ISM is focused on federal agencies, it is mapped to the Practice Guide because of its flagship status on Australian cybersecurity.

4.2.9 Information Security Management Guidelines: Risk Management of Outsourced ICT Arrangements

Information Security Management Guidelines: Risk Management of Outsourced ICT Arrangements (Including Cloud), authored by Australia's Attorney-General's Department, is intended for government agencies. While much of the information included in this document may benefit any organization considering cloud services, it is tailored to government needs only. Also, it is primarily aimed at the organizational and policy levels. Thus, it is not included in the mapping of the Practice Guide.

4.2.10 Information Security Registered Assessors Program (IRAP)

IRAP is an ASD initiative to ensure that individuals conducting cybersecurity assessments have an appropriate skill level to produce consistent quality. IRAP is not a standard, though it is often mistaken to be such; rather, it demonstrates that IRAP members have attained the experience, security certifications, and technical understanding to independently assess systems against the ISM and Protective Security Policy Framework. This program is especially important for entities that desire to provide IT services to Australian government agencies (and increasingly adopted by state and territory governments) due to the ASD's recommendation of compliance with IRAP before procurement. IRAP is included on the list of identified "standards" as MITRE research found it frequently referenced, at times, as if it were a standard. IRAP leverages the ISM as a basis for assessment of technical controls for services that go through the accreditation process. It does not apply in the context of mobile device security for SMEs. Because it is not an actual standard and applies only to government or entities opting in to IRAP, it is not mapped to the Practice Guide.

4.2.11 Privacy Guidelines

The Office of the Australian Information Comminssioner's (OAIC) *Guide to Securing Personal Information* provides technical guidelines that businesses can use to comply with the Australian Privacy Principles requirements [25]. This research uses the *Guide to Securing Personal Information* as a basis for mapping to the guidelines found in the Practice Guide. It is important to note that this mapping is limited to the extent that the findings and recommendations from the OAIC guidelines are limited to personal information and that the Practice Guide includes any data. Additionally, the OAIC guide includes specific reference to mobile devices that were not

included in the mapping in this report. General guidelines are provided for businesses to adopt policies regarding the use of mobile devices, including the separation of business and personal data, password protection, and an awareness program for employees regarding the risks of using personal devices for business activities.

While the OAIC guide is beneficial to organizations with mobile devices, it lacks the technical specificity necessary for mapping to the Practice Guide. Additionally, the *Guide to Securing Personal Information* refers to the OAIC's "Mobile Privacy—A Better Practice Guide for Mobile App Developers" [26]. While useful for entities that develop mobile applications within their own organizations, the Practice Guide used mobile applications provided by commercial vendors and therefore did not include any mobile application development recommendations for privacy protection. For the purposes of the project, it is assumed that most SMEs will be users of mobile applications and not developers of mobile applications. However, in circumstances where Australian organizations, particularly start-ups, develop applications to support their businesses, this guide is useful.

5 Laws, Standards, and Guidelines Mapping

MITRE analyzed the laws, standards, and guidelines identified in Section 4 of this report and determined that three of the documents were directly relevant to mobile device security guidelines contained within the Practice Guide. This section provides a detailed analysis showing how the most relevant Australian laws, standards, and guidelines map to the Practice Guide. It includes tables that illustrate how specific controls found in the Australian documents align to comparable elements within the Practice Guide. For example, in Table 2, which compares the ISM to the Practice Guide, the Security Characteristic column identifies elements from the Practice Guide that are needed to reduce the risk from mobile devices storing or accessing enterprise data. The Example Capability column, taken from the Practice Guide, identifies technical features that can be applied to address the accompanied security characteristic. The final column, Information Security Manual Control, shows how technical controls align to the Practice Guide's corresponding security characteristics.

This section also uses visual representations to make the mapping easy to understand. We began by identifying the six security characteristics from the Practice Guide and representing them as hexagons in a heat map. The color of each hexagon represents the degree of overlap between the Australian document and the Practice Guide. In the ISM mapping, green denotes that the Practice Guide security characteristic was mapped to five or more ISM controls while yellow represents that one to four controls have been mapped. In the Essential Eight and Privacy Law mapping, green denotes that a security characteristic was mapped to two or more guidelines, while yellow represents a mapping to one guideline. In all cases, red denotes that the security characteristic was not mapped to a control or guideline, thus signifying a gap.

5.1 Information Security Manual

This section maps the ISM Control Manual to guidelines found in the Practice Guide.

The Australian Government ISM Control Manual provides a comprehensive view of cybersecurity and addresses IT security controls, governance, physical security, personnel security, and other aspects of an organizational risk management program. The IT security controls that are most relevant for mobile security were found in the Working Off-Site section of the ISM, so our comparison primarily focuses on controls from that section of the report. Overall, our analysis found that the Practice Guide mapped nicely to ISM controls.

Table 2-ISM to Practice Guide Security Characteristic Mapping

Security Characteristic	Example Capability	Information Security Manual Control
Data Protection	protected storage: device encryption, secure containers, trusted key storage, hardware security modules, remote wipe; protected communications: virtual private network (VPN), to include per-app VPN; data protection in process: encrypted memory, protected execution environments	**0869, 1085, 0864, 0705, 0700, 0701, 0702, 1345**
Data Isolation	virtualization, sandboxing, memory isolation, trusted execution, device resource management, data flow control, data tagging, baseband isolation	**1047**
Device Integrity	baseband integrity checks, application black/whitelisting; device integrity checks: boot validation, application verification, verified application and OS updates, trusted integrity reports, policy integrity verification	**1399, 1367**
Monitoring	canned reports and ad-hoc queries, auditing and logging, anomalous behavior detection, compliance checks, asset management, root and jailbreak detection, geofencing	**0862, 0863**
Identity and Authorization	local user authentication to applications, local user authentication to device, remote user authentication, remote device authentication, implementation of user and device roles for authorization, credential and token storage and use, device provisioning and enrollment	**ISM controls not mobile specific**
Privacy Protection	informed consent of user, data monitoring minimization, privacy notification provided to user	**ISM controls not mobile specific**

Green denotes that the Practice Guide security characteristic was mapped to five or more ISM controls, while yellow represents that one to four controls have been mapped. Red denotes the security characteristic was not mapped to the control or guideline, thus signifying a gap.

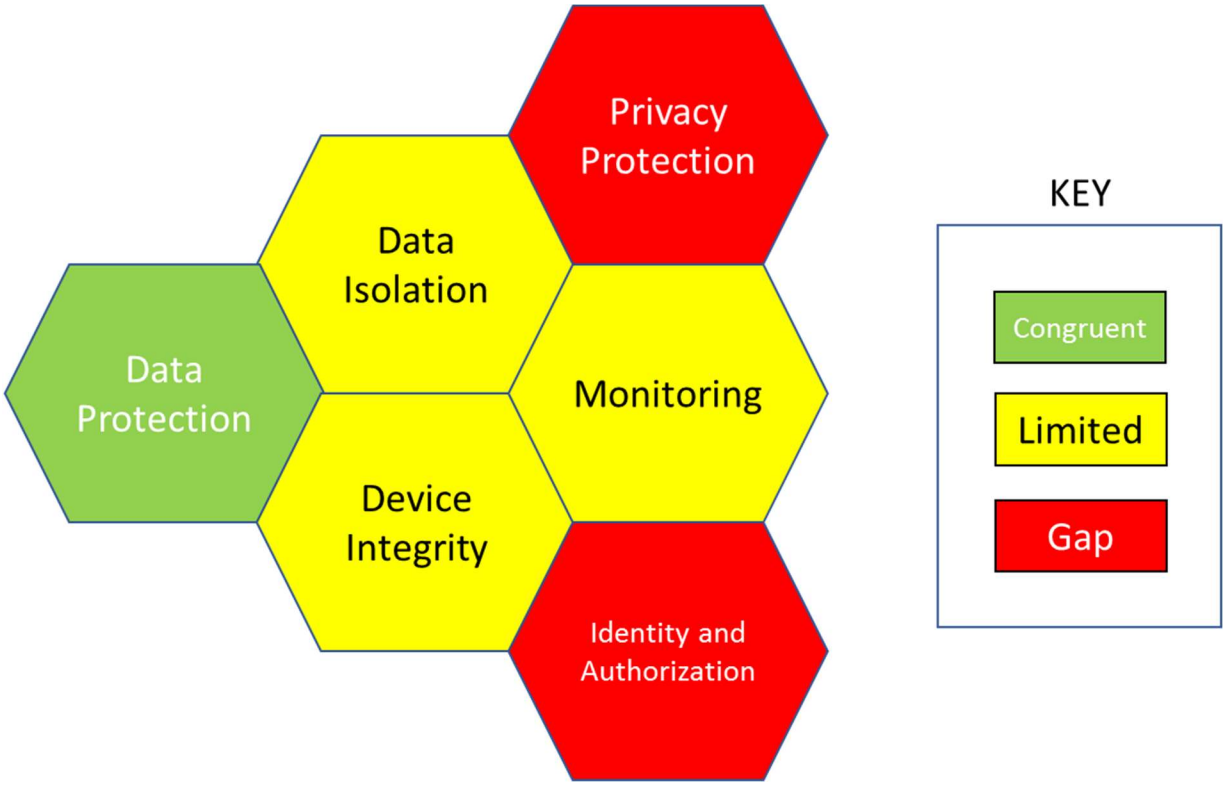


Figure 1 ISM Control Mapping

The following sections provide more detailed explanations of each security characteristic mapping to the ISM. A summary of each mapped ISM control and its applicability to the Practice Guide is provided in the narrative.

5.1.1 Key Findings

The ISM and the Practice Guide align in the use of encryption, in enabling device security functions, and in the ability to destroy data on lost devices. Additionally, the Practice Guide provides some alignment with the ISM on device integrity and the need for audit and monitoring. The Practice Guide exceeds the ISM controls by addressing the identity and authorization and privacy protection security characteristics in the mobile context. While these topics are addressed by the ISM from an enterprise level, the Practice Guide provides specific practical implementations of these characteristics that directly affect mobile device usage.

Personnel awareness (Control 1083), however, is not addressed by the Practice Guide. Australian organizations that attempt to implement the Practice Guide should take steps to make device owners aware of the activities that are permitted for data communications. For example, an organization may want to inform personnel that communicating sensitive budget data over

insecure transport such as short message service (SMS) is inappropriate. Further, the use of privacy filters or screens as a method to dissuade shoulder surfing is not included in the Practice Guide as a threat mitigation tactic. The Practice Guide attempts to find a reasonable balance between security and user functionality. As such, the use of screen filters was not included in the Practice Guide because it minimally reduces the threat surface while simultaneously having a negative effect on mobile device functionality due to reduced screen viewing area.

The ISM Control Manual encourages adopting organizations to ensure that the carrier service can provide security updates to the mobile device as soon as they become available. This is an important consideration for organizations, especially those that rely on Android devices. Updates to the Android operating systems are typically delivered through the carrier that provides service to the device [27]. This can lead to unreasonable delay in receiving important security updates. The Practice Guide does not incorporate this risk into the guidelines, but it is advisable for adopting organizations to assess this risk.

A final observation is that some of the gaps identified between the ISM and the Practice Guide are largely due to the difference in the intended audience. The intended audience for the Practice Guide is industry rather than government. The Practice Guide attempts to provide practical, real-world security guidelines that most organizations can adopt rather than bespoke solutions that a federal agency charged with protecting classified data requires.

5.1.2 Technical findings

Data Protection

ISM Control 0869 directs the use of cryptographic protection on all mobile devices utilized by an organization. This is directly addressed by the Practice Guide with a device-level encryption policy that recommends using the file encryption on mobile device capability, which employs Federal Information Processing Standards (FIPS) 140-2–approved cryptographic modules.

Control 1085 directs the use of encryption over public communication mechanisms for sensitive or classified information. The Practice Guide does not address any classified data but does recommend data-in-transit encryption for all communications over untrusted networks. The Practice Guide documents the use of transport layer security (TLS) for all communications to cloud services and on-premises components.

Control 0864 directs agencies to prevent device owners from disabling security functions once provisioned. For example, if a security policy disables the use of the camera, the device user should not be able to circumvent the control and activate the camera. This control is directly addressed in the Practice Guide and involves using a mobile device management (MDM) capability built into the mobile operating system. The mobile operating system prevents any modification of security policy by the device user when under management.

Controls 0705 and 1345 disable the use of VPN split tunneling on devices when the mobile device is capable of such a configuration. Split tunneling could potentially allow an attacker from an unsecured network to infiltrate a secure VPN connection. The architecture described in the Practice Guide does not allow the use of split tunneling when accessing organizational resources by the established network security policies and a lack of VPN exercised within the architecture.

Controls 0700, 0701, and 0702 all relate to the ability to destroy data that resides on the device in an emergency. This functionality is supported in the Practice Guide through the remote wipe capability within the MDM. When executed, remote wipe renders access to enterprise data infeasible through cryptographically secure processes.

Data Isolation

ISM Control 1047 mandates the use of a technical means to separate sensitive organization-owned data from any personal information that is stored on the mobile device. This functionality is described in the Practice Guide: Use native operating system process isolation techniques that prevent applications from accessing, gathering, or modifying information from other applications.

Device Integrity

ISM Control 1399 permits the use of personally owned mobile devices only when the configuration of the mobile device meets security policy. This is supported by the Practice Guide cloud-only architecture through the deployment of mobile threat detection (MTD) on the mobile endpoint. The MTD client has the capability of reporting device integrity status (such as if the device has been rooted or jailbroken) to an administrator. IT security personnel can revoke access to organization resources if the MTD client reports that a mobile device is out of compliance.

Control 1367, similar to control 1399, directs the use of a security policy enforcement capability when the mobile device is organizationally owned. The Practice Guide hybrid architecture satisfies this requirement by using MDM capabilities. IT security personnel can revoke access to organizational resources when the MDM reports noncompliance of a mobile device.

Monitoring

Controls 0862 and 0863 recommend regular auditing and configuration control of mobile devices –in the same manner as devices in an office environment–as a method to ensure that the state of security on the mobile device has not degraded over time. As mentioned in previous sections, the use of an MDM will apply technical controls to a mobile device that complies with organizational security policy, but regular monitoring is essential to detect abnormalities that represent a coordinated attack. The hybrid architecture in the Practice Guide addresses this requirement by deploying a systems management software product in the enterprise. The solution can deploy configuration controls for both traditional workstation endpoints and mobile devices through one administrative console. Similarly, hardware and software inventories are available for audit through the systems management solution.

Identity and Authorization

The ISM control manual coverage of identity and authorization security characteristics is at an enterprise level and is not mobile specific. Specifically, the ISM Control Manual's Access Control section is geared toward the management of traditional PCs rather than mobile device controls such as the use of authentication methods to unlock the mobile device.

Privacy Protection

The ISM control manual coverage of privacy security characteristics is not mobile specific.

5.2 Essential Eight

This section maps ASD's Strategies to Mitigate Cyber Incidents, Essential Eight, to guidelines found in the Practice Guide.

The following table decomposes ASD's Essential Eight into requirements to facilitate mapping to the security characteristics in the Practice Guide. The Identifier column provides a shorthand notation for each Essential Eight requirement in the second column. As noted in the ISM, some technologies (such as mobile devices) may lack the functionality to feasibly implement the Essential Eight. In such cases and in this mapping exercise, implementing the Essential Eight on mobile devices can be achieved by using controls that meet the general principles behind the Essential Eight [24].

Table 3-Essential Eight Requirements

Identifier	Essential Eight Requirement
EE-1	Application whitelisting: A whitelist only allows selected software applications to run on computers.
EE-2	Patch applications: A patch fixes security vulnerabilities in software applications.
EE-3	Disable untrusted Microsoft Office macros: Microsoft Office applications can use software known as macros to automate routine tasks.
EE-4	User application hardening: Block web browser access to Adobe Flash Player (uninstall if possible), web ads, and untrusted Java code on the internet.
EE-5	Restrict administrative privileges: Only use administrator privileges for managing systems, installing legitimate software, and applying software patches. These should be restricted to only those who need them.
EE-6	Patch operating systems: A patch fixes security vulnerabilities in operating systems.
EE-7	Multifactor authentication: This is when a user is granted access only after successfully presenting multiple, separate pieces of evidence—typically something you know, like a pass phrase; something you have, like a physical token; and/or something you are, like biometric data.
EE-8	Daily backup of important data: Regularly back up all data and store it securely offline.

Table 4 maps the requirements above to the security characteristics found in the Practice Guide.

Table 4-Essential Eight Requirements to Practice Guide Security Characteristic Mapping

Security Characteristic	Example Capability	Essential Eight Requirement
Data Protection	protected storage: device encryption, secure containers, trusted key storage, hardware security modules, remote wipe; protected communications: virtual private network (VPN), to include per-app VPN; data protection in process: encrypted memory, protected execution environments	**EE-5, EE-6**
Data Isolation	virtualization, sandboxing, memory isolation, trusted execution, device resource management, data flow control, data tagging, baseband isolation	**EE-4**
Device Integrity	baseband integrity checks, application black/whitelisting; device integrity checks: boot validation, application verification, verified application and OS updates, trusted integrity reports, policy integrity verification	**EE-1, EE-2, EE-6**
Monitoring	canned reports and ad-hoc queries, auditing and logging, anomalous behavior detection, compliance checks, asset management, root and jailbreak detection, geofencing	**No mapping exists to Essential Eight requirements**
Identity and Authorization	local user authentication to applications, local user authentication to device, remote user authentication, remote device authentication, implementation of user and device roles for authorization, credential and token storage and use, device provisioning and enrollment	**EE-7**
Privacy Protection	informed consent of user, data monitoring minimization, privacy notification provided to user	**No mapping exists to Essential Eight requirements**

Green denotes that the Practice Guide security characteristic was mapped to two or more requirements, while yellow represents a mapping to one requirement. Red denotes that the security characteristic was not mapped to any requirements, thus signifying a gap.

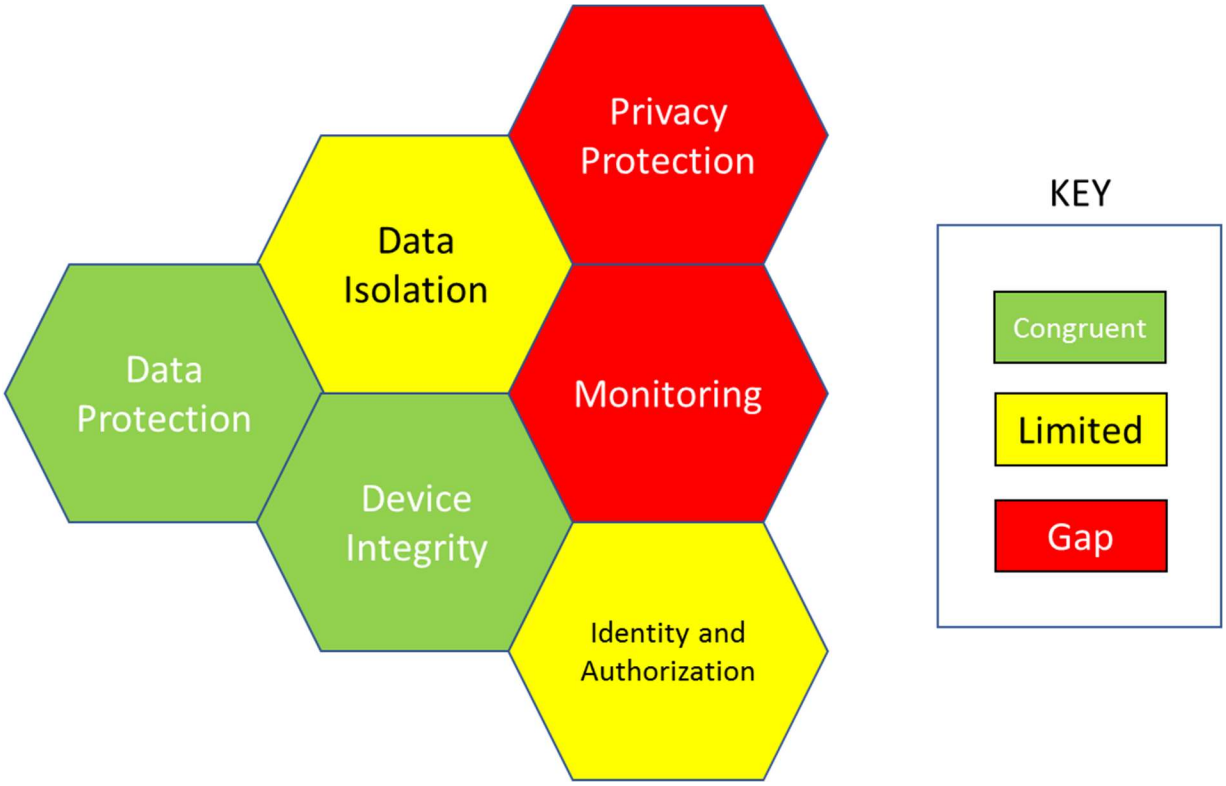


Figure 2 Essential Eight Mapping

5.2.1 Key Findings

Australian organizations adopting the Practice Guide have the baseline strategies of the Essential Eight addressed by the cloud and hybrid architectures. The Practice Guide security characteristics address six of the eight Essential Eight requirements. Data protection, data isolation, device integrity, and identity and authorization mechanisms provided in the Practice Guide align with Essential Eight requirements. The remaining requirements "disable untrusted Microsoft Office macros" and "daily backup of important data" were deemed out of scope in the mobile security context. Microsoft Office macros are not used in a mobile operating system environment and therefore are not applicable. Backup of critical data is best addressed through a nonmobile-specific enterprise policy for data retention and/or by leveraging the benefits of cloud technologies. Further, the Practice Guide architectures would address the monitoring security characteristic, which goes beyond the strategies of the Essential Eight.

The architecture described in the Practice Guide enables the use of BYOD, company owned personally enabled (COPE), and other mobile device deployment models, but none are specifically addressed in the Essential Eight. ASD's publication *Risk Management of Enterprise Mobility Including Bring Your Own Device* addresses BYOD through the discussion of business cases but does not provide practical how-to guidance that SMEs could potentially adopt quickly within their own organization.

5.2.2 Technical Findings

Data Protection

Requirement EE-5 in the mobile context is supported by the Practice Guide through the implementation of an MDM. Organization administrators can take actions on the mobile device that require elevated privileges, such as applying security restrictions, through the MDM. Mobile operating systems further ensure the legitimacy of remote MDM administrative commands by verifying the integrity through cryptographic methods.

Requirement EE-6 in the mobile context is supported by the Practice Guide through the guidance for organizations to keep mobile devices regularly updated to receive the latest preventive measures against vulnerabilities. The architecture also allows for a policy that blocks access to organizational resources when the mobile device lacks the latest OS patch level.

Data Isolation

Requirement EE-4, user application hardening, is not directly addressed in the Practice Guide. Mobile application development best practices were deemed out of scope to include in the currently published version of the Practice Guide. However, application-level policies documented in the Practice Guide architecture disable attachments of email messages, which attackers can use to distribute malware to mobile devices, thereby isolating the malicious email attachment from the rest of the data on the device.

Device Integrity

Requirement EE-1, application whitelisting, is supported by the Practice Guide hybrid architecture through managed applications. Managed applications are specially compiled applications where security controls are applied that comply with an organization's policy. The MDM allows an administrator to deploy managed applications to the organization by either requiring the installation, making it optional, or marking it not applicable. These options give an organization the ability to allow, or whitelist, only approved applications. The Practice Guide used this functionality to seamlessly distribute an email application to mobile devices regardless of hardware platform.

Requirements EE-2 and EE-6, application and operating system patch updates, are supported by the Practice Guide by using ecosystem-specific integrity checks via cryptographically protected applications. Mobile application stores require the developer to digitally sign the software update (or patch) with a trusted cryptographic key before uploading to the application store. The mobile device also verifies the digital signature of application and operating system updates before final installation. These actions prevent attackers from modifying software patches to include malware or other exploits.

Monitoring

No Essential Eight requirements directly map to this Practice Guide security characteristic. Organizations seeking Australia-specific guidelines on monitoring need to go through the ISM (noting this is limited, as discussed above) or other sources.

Identity and Authorization

Requirement EE-7, multifactor authentication, is not directly supported by the documented Practice Guide architectures, but the capability exists. The hybrid architecture uses identity federation services to link the device owner's identity to cloud organizational resources. This linkage requires the device owner to authenticate by using an enterprise password before accessing organizational resources. However, a multifactor authentication scheme could be implemented with additional configuration.

Privacy Protection

No Essential Eight requirements directly map to this Practice Guide security characteristic. Organizations seeking Australia-specific guidelines need to obtain information from another source.

5.3 Privacy Laws

This section maps Australian Information Commissioner's *Guide to Securing Personal Information* [8] to guidelines found in the Practice Guide. The following table decomposes the Office of the Australian Information Commissioner's *Guide to Securing Personal Information* [8] into requirements to facilitate mapping to the security characteristics in the Practice Guide. The requirements table does not represent the *Guide to Securing Personal Information* in its entirety; rather, it uses the Information and Communication Technology Security section as a basis. The Identifier column provides a shorthand notation for each ICT Requirement in the second column.

Topics such as governance were deemed out of scope for comparison to guidelines found in the Practice Guide. However, the *Guide to Securing Personal Information* describes the security characteristics of cloud services that an organization should consider when storing personal information remotely in the cloud. These considerations are important for any organization that adopts either of the reference architectures in the Practice Guide because of the dependence of cloud services for email and mobile device management. Dependence of Australian organizations on cloud and mobile platforms was confirmed by MITRE's consultation effort for this project.

For example, the OAIC guide recommends verifying security controls of a cloud service provider to a sufficient level of detail, such as through independent testing and validation. An organization adopting the Practice Guide architecture could satisfy this OAIC recommendation by reviewing the audit reports available on the Microsoft Azure (the cloud platform that supports Intune and Office365 practice guide products) website [27].

Table 5-ICT Requirements Table

Identifier	ICT Requirement
ICT-1	It is expected that entities regularly monitor the operation and effectiveness of their ICT security measures to ensure that they remain responsive to changing threats and vulnerabilities and other issues that may affect the security of personal information.
ICT-2	You should be aware of the personal information you hold on your ICT system and where it is located.
ICT-3	Your ICT security measures should ensure that all of your systems are secure and that they provide a safe environment for your staff to carry out your business.
ICT-4	Your ICT security measures should ensure that all of your systems are secure and that they provide a safe environment for your customers to interact with your agency or business, for example, when they make payments or provide their banking details and/or other personal information.
ICT-5	ICT security measures help mitigate the risks of internal and external attackers and the damage caused by malicious software such as malware, computer viruses, and other harmful programs.
ICT-6	You need to consider the security of all systems that use or interact with your ICT system. This includes securing your website(s), social media platforms, and mobile device applications (apps).
ICT-7	As well as ICT security against external and internal threats, it is important to consider the possibility of human error (for example, misplacing devices such as laptops and data storage devices, noting that encryption and password protection can mitigate this risk).
ICT-8	As well as ICT security against external and internal threats, it is important to consider the possibility of hardware or software malfunctions.
ICT-9	As well as ICT security against external and internal threats, it is important to consider the possibility of power failure.
ICT-10	As well as ICT security against external and internal threats, it is important to consider the possibility of system failure caused by natural disasters such as earthquakes, floods, and extreme weather conditions.

Table 6 maps the requirements above to the security characteristics found in the Practice Guide.

Table 6 ICT Requirements to Practice Guide Security Characteristic Mapping

Security Characteristic	Example Capability	ICT Requirement
Data Protection	protected storage: device encryption, secure containers, trusted key storage, hardware security modules, remote wipe; protected communications: virtual private network (VPN), to include per-app VPN; data protection in process: encrypted memory, protected execution environments	**ICT-5, ICT-7**
Data Isolation	virtualization, sandboxing, memory isolation, trusted execution, device resource management, data flow control, data tagging, baseband isolation	**ICT-5**

Device Integrity	baseband integrity checks, application black/whitelisting; device integrity checks: boot validation, application verification, verified application and OS updates, trusted integrity reports, policy integrity verification	**ICT-5**
Monitoring	canned reports and ad-hoc queries, auditing and logging, anomalous behavior detection, compliance checks, asset management, root and jailbreak detection, geofencing	**ICT-1**
Identity and Authorization	local user authentication to applications, local user authentication to device, remote user authentication, remote device authentication, implementation of user and device roles for authorization, credential and token storage and use, device provisioning and enrollment	**ICT-7**
Privacy Protection	informed consent of user, data monitoring minimization, privacy notification provided to user	**No mapping exists to ICT requirements**

Green denotes that the Practice Guide security characteristic was mapped to two or more requirements, while yellow represents a mapping to one requirement. Red denotes that the security characteristic was not mapped to any requirements, thus signifying a gap.

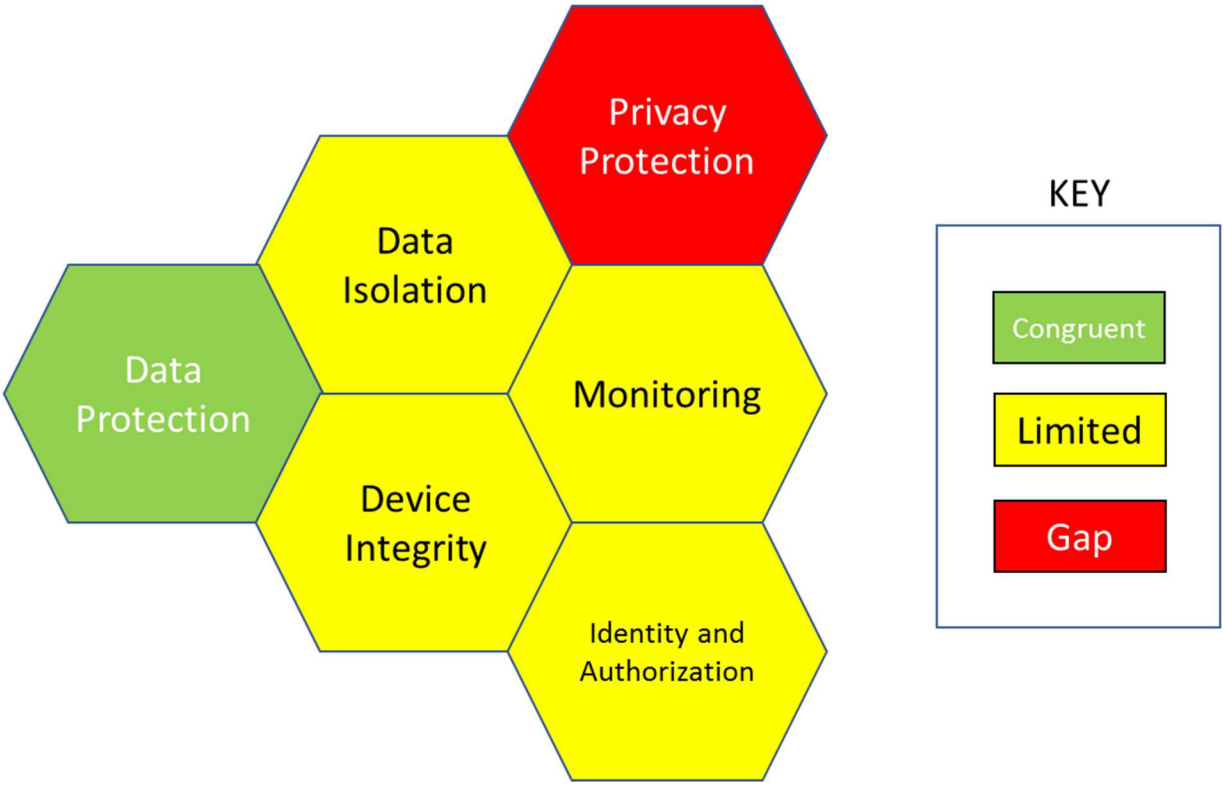


Figure 3 Guide to Securing Personal Information Mapping

5.3.1 Key Findings

The only government regulation that has a nationwide, direct effect on Australian organizations implementing a mobile device security program is the Privacy Amendment (Notifiable Data Breaches) Act 2017. The recent introduction of the Privacy Amendment (Notifiable Data Breaches) Act 2017 will require organizations with obligations under the Privacy Act 1988 to comply with data protection regulations when handling personal information [28]. Australian organizations should consider the effect of mobile device usage within their organization when handling personal consumer data, and more broadly, the Australian Privacy Principles.

The ICT requirements if adapted for the mobile environment provide broad coverage of the security characteristics described in the Practice Guide. One characteristic that is covered in the Practice Guide but not addressed specifically by the ICT is privacy protection. It is worth noting that the focus of the Practice Guide is on specific security controls and standards that support privacy, for example, by enabling confidentiality of data. Such detailed controls and standards are often missing from government regulations or guidelines, which is not necessarily an issue if the goal of such documents is to provide high-level direction rather than specific technical guidelines. For this reason, companies following the ICT requirements would need to augment

that information with practical mobile-specific guidelines that address the challenges faced when implementing a secure mobile program. Conversely, the Practice Guide does not address four ICT requirements that relate to IT governance because they are out of scope for this particular Practice Guide.

5.3.2 Technical Findings

Data Protection

ICT-5 and ICT-7 are broad requirements to ensure that security measures are in place to protect against external and internal threats. These requirements cite a need for protection against malicious software and human error, both of which apply to mobile devices. The Practice Guide architectures (cloud-only and hybrid) protect against malicious software (more commonly referred to as malware in a mobile context) with the deployment of an MTD client on the mobile device as a requirement before the device owner is permitted to access organizational resources. In addition, the Practice Guide describes the use of device ecosystem–provided application store malware detection tools (e.g., Google Play Protect) that scan applications from developers as applications are uploaded, which prevents the spread of malware to end users. Human error, such as the device owner losing the mobile device, is protected against by use of an MDM. With appropriate organizational policy, the device owner is required to report a missing device to the appropriate personnel. The MDM administrator is then able to take actions such as wiping or physically locating the phone through features of the MDM.

Data Isolation

The Practice Guide architectures protect against mobile malware (ICT-5) by using common operating system techniques. Process isolation prevents malware on the mobile device from accessing, gathering, or modifying information from other legitimate applications. Trust execution environments further isolate sensitive operations from malware on the device.

Device Integrity

The Practice Guide architectures protect against mobile malware (ICT-5) by using device-specific integrity checks such as operating system boot validation, cryptographically protected application, and operating system updates. The first technique blocks the execution of the operating system when modifications have been detected. The use of cryptographically protected applications and operating system updates increases the difficulty of an attacker to distribute mobile malware.

Monitoring

Requirement ICT-1 uses regular monitoring of systems as a method to detect threats and vulnerabilities that may provide an attacker a vector to access, gather, or modify personal data. The Practice Guide hybrid build supports this requirement through automated alerts that are sent to designated personnel when policy violations occur, such as when malware is detected on the device. The mobile device can then be remotely wiped or other actions performed as organizational policy dictates.

Identity and Authorization

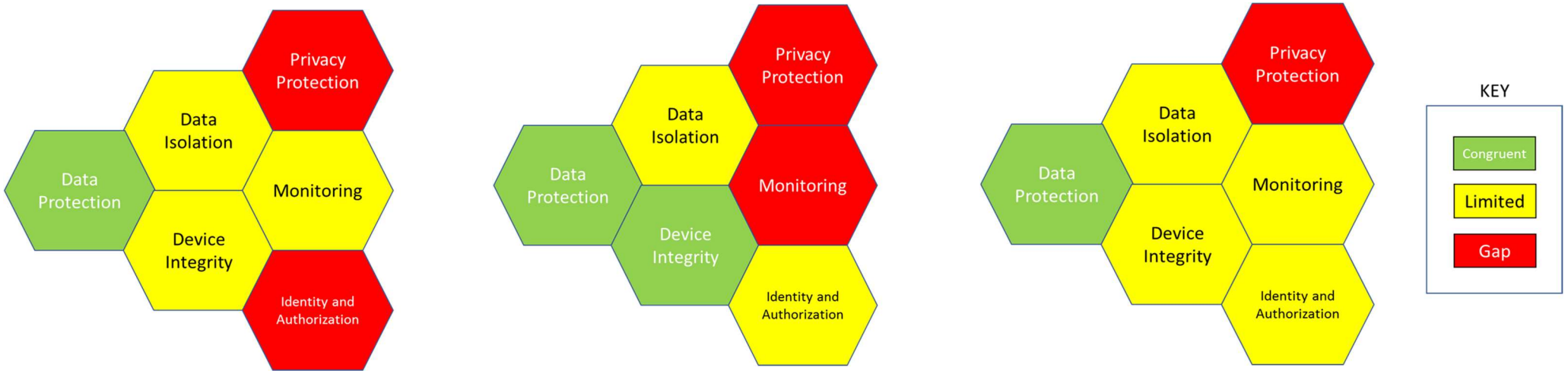
Requirement ICT-7 suggests the use of passwords as a mechanism to protect against human error, such as when a device is lost by the device owner. The Practice Guide cloud-only and hybrid builds support this requirement through enforcement of an MDM policy that requires the device user to set a pass code needed to unlock the device. The device automatically locks after a configured number of attempts and can be unlocked only by administrator action. At an application level, the hybrid build further requires an enterprise password to access resources such as email, calendar, and contacts.

Privacy Protection

No ICT requirements directly map to this Practice Guide security characteristic. This is discussed further below.

5.4 Mapping Overview

A diagram summarizing MITRE's mapping of key Australian mobile security guidelines to the Practice Guide is provided in Figure 4. Three of the six security controls—data protection, data isolation, and device integrity—were addressed by all three Australian documents to some extent. One of the controls, monitoring, was addressed only by the ISM. Another control, identity and authorization, was addressed by the Essential Eight and ICT guidelines but not in the ISM. The privacy protection security control was found to be a gap across all three Australian guidelines. In addition, privacy on mobile devices can be achieved by implementing other technical security controls. For example, in the Practice Guide, privacy protection as a security control includes informed consent of user, data monitoring minimization, and privacy notification provided to user.



ISM Control Mapping

Essential Eight Mapping

Guide to Securing Personal Information Mapping

Figure 4 Security Control Mapping Comparison

6 Findings and Recommendations

Many organizations in Australia, most notably SMEs, have little understanding of the risks they face when using mobile devices. Some companies who do attempt to address these risks struggle to find relevant laws, standards, and guidelines that are easy to understand and implement. This is further complicated by the fact that guidelines produced by government agencies across the federal and state levels are often inconsistent. For example, there is often confusion about what steps are mandatory and which actions are voluntary. In addition, some of the guidelines related to cybersecurity that can be applied to mobile devices lead to stringent security controls that exceed the level of security necessary for many enterprises, especially for SMEs.

MITRE's assessment found that out of 47 security regulations, laws, standards, and guidelines, three are particularly relevant and useful for mobile device security: ASD's *Information Security Manual*, ASD's Essential Eight, and the OAIC's *Guide to Securing Personal Information*. By mapping the Practice Guide to those three documents, MITRE was able to identify strengths, weaknesses, overlaps, and gaps. For example, our analysis found that the ISM mobile security controls and the Essential Eight were the most relevant to Australian organizations in part due to procurement processes that reference these documents.

Our analysis also showed that the Practice Guide provided useful and practical guidelines on the specific issue of mobile device security within the Australian ecosystem. The Practice Guide finds a reasonable balance between security and user functionality, which works well for Australian organizations.

At present, the Practice Guide can be a useful adjunct to the existing set of Australian guidelines and could serve as a preeminent and comprehensive reference for organizations seeking to improve the cybersecurity of mobile devices. Furthermore, MITRE's analyses and consultations with industry revealed that, with several modifications, the Practice Guide could become even more useful for SMEs:

- Simplify the Practice Guide's technical language to make the report more accessible to a wider audience, especially SMEs employing BYOD policies. Use infographics where appropriate.

- Include mobile security best practices and concrete examples in the Practice Guide.

- Discuss the benefits and limitations of using cloud-based solutions that provide built-in security for SMEs relying on mobile devices for core business functions.

- Include a deeper discussion of the touchpoints between security and privacy. For example, the Guide could provide more information on the risks and benefits of storing data on a mobile device versus saving it in a cloud. While the Practice Guide discusses the use of encryption for data in transit, it could tailor that discussion to address easy-to-implement approaches for SMEs. It could also include guidelines on encryption for data at rest.

Organizations attempting to secure mobile devices must sift through a lengthy list of possible laws, regulations, standards, and guidelines to discern what steps they must take and what actions are recommended as best practices. The Australian government can begin to address this issue by harmonizing the guidelines it provides to industry. In this area, Australia could learn from the United States' experience in consolidating multiple competing government compliance frameworks, most notably the Department of Defense's transition from the Defense Information Assurance Certification and Accreditation Process to the NIST Cybersecurity Framework. One benefit of using the Practice Guide is that it is based on that same framework, which is gaining significant traction globally [29], including within Australia.

This study only scratched the surface of this complex issue by mapping specific controls in three documents to those in the Practice Guide. Further analyses of this type could yield important insights into the overlaps and gaps that organizations face in following the multiple cybersecurity requirements and guidelines emanating from government.

MITRE recommends that AustCyber, as a government-funded and industry-facing independent entity, take the lead in facilitating intergovernmental and multistakeholder discussions on cybersecurity standards harmonization with mobile device security serving as the initial use case because of its broad applicability across both SMEs and larger enterprises.

Appendix A NIST Special Publication 1800-4 Security Control Map

The table below is the original mapping of practice guide security characteristics to the NIST Cybersecurity Framework, NIST Special Publication 800-53 controls, ISO 27002 and the Council on Cybersecurity's Critical Security Controls for Effective Cyber Defense.

Example Characteristic		Cybersecurity Standards and Best Practices					
Security Characteristic	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST SP 800-53 rev4**	**IEC/ISO 27002**	**CAG20**
Data Protection	protected storage: device encryption, secure containers, trusted key storage, hardware security modules, remote wipe; protected communications: virtual private network (VPN), including per-app VPN; data protection in process: encrypted memory, protected execution environments	Protect	Data Security, Protective Technologies	PR.DS-1 PR.DS-2 PR.DS-5 PR.PT-4	AC-20, AU-9, IA-6, IA-7, MP-6, SA-13, SC-8, SC-11, SC-12, SC-13, SC-17, SI-12	6.2.1 9.4.3 9.4.4 9.4.5 10.1.2 12.4.2 12.4.3 13.1.1 13.2.1 13.2.3 14.1.3	CSC-15
Data Isolation	virtualization, sandboxing, memory isolation, trusted execution, device resource management, data flow control, data tagging, baseband isolation	Protect	Data Security, Protective Technologies	PR.DS-1 PR.DS-5 PR.PT-3	CM-11, SA-13, SC-3, SC-11, SC-35, SC-39, SC-40, SI-16	6.2.1 6.2.2 9.4.1 9.4.4 12.2.1	CSC-7 CSC-12 CSC-14
Device Integrity	baseband integrity checks, application black/whitelisting; device integrity checks: boot validation, application verification, verified application and OS updates, trusted integrity reports, policy integrity verification	Protect, Detect	Data Protection, Anomalies and Events, Security Continuous Monitoring	PR.DS-6 DC.CM-4 DE.CM-5 DE.CM-6	AC-20, CM-3, IA-3, IA-10, SA-12, SA-13, SA-19, SC-16, SI-3, SI-4, SI-7	6.2.1 12.2.1 14.2.4 15.1.3	CSC-3 CSC-6 CSC-12

Monitoring	canned reports and ad-hoc queries, auditing and logging, anomalous behavior detection, compliance checks, asset management, root and jailbreak detection, geofencing	Identify, Protect, Detect	Asset Management, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes	ID.AM-1 ID.AM-2 PR.DS-3 PR.MA-2 PR.PT-1 DE.AE-1 DE.AE-1 DE.AE-3 DE.AE-5 DE.CM-1 DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.CM-7 DE.CM-8 DE.DP-2 DE.DP-4	AC-2, AC-3, AC-7, AC-21, AC-25, AU-3, AU-5, AU-5, AU-7, AU-8, AU-9, AU-10, AU-12, AU-13, AU-14, AU-15, AU-16, CA-7, CM-2, CM-3, CM-6, CM-8, CM-11, IA-4, IR-4, IR-5, IR-7, IR-9, MA-6, SA-13, SA-22, SC-4, SC-5, SC-7, SC-18, SC-42, SC-43, SI-3, SI-4, SI-5	6.1.4 6.2.1 6.2.2 8.1.1 8.1.2 9.2.3 9.2.5 9.4.4 9.4.5 10.1.2 12.2.1 12.4.1 12.4.2 12.4.3 12.5.1 12.6.1 12.7.1 13.1.1 15.1.3 16.1.2 16.1.4 16.1.5 18.2.3	CSC-1 CSC-2 CSC-5 CSC-6 CSC-10 CSC-11 CSC-12 CSC-13 CSC-14 CSC-18

Identity and Authorization	local user authentication to applications, local user authentication to device, remote user authentication, remote device authentication, implementation of user and device roles for authorization, credential and token storage and use, device provisioning and enrollment	Protect, Detect	Access Control, Protective Technologies, Asset Management	ID.AM-1 PR.AC-1 PR.AC-3 PR.AC-4 PR.PT-3 DE.CM-3 DE.CM-7	AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-16, AC-17, AC-18, AC-19, AC-20, AU-16, CM-5, CM-7, IA-2, IA-3, IA-5, IA-6, IA-7, IA-8, IA-9, IA-11, MP-2, SA-9, SA-13, SA-19, SC-4, SC-16, SC-40	6.2.1 6.2.2 9.1.1 9.1.2 9.2.1 9.2.2 9.2.3 9.2.4 9.3.1 9.4.1 9.4.2 9.4.3 13.1.1 13.1.2 13.2.2 13.2.3 14.1.2 14.1.3	CSC-8 CSC-9
Privacy Protection	informed consent of user, data monitoring minimization, privacy notification provided to user	Identify, Protect	Governance, Training and Awareness	ID.GV-3 PR.AT-1	AR-4, AR-7, DM-1, IP-1, IP-2, SE-1, TR-1, UL-1	18.1.4	CSC-17

Appendix B NIST Special Publication 1800-4 Australian Privacy Principles Coverage

The table below presents the applicability of Australian Privacy Principles to the Mobile Device Security Practice Guide.

Principle	Sub Principle	1800-4 Coverage
Australian Privacy Principle 1—open and transparent management of personal information	Compliance with the Australian Privacy Principles, etc.	Not Applicable
	APP privacy policy	Partial Applicability
	Availability of APP privacy policy, etc.	Applicable
Australian Privacy Principle 2—anonymity and pseudonymity	Option of not identifying or use of a pseudonym	Not Applicable
Australian Privacy Principle 3—collection of solicited personal information	Personal information other than sensitive information	Applicable
	Sensitive information	Applicable
	Means of collection	Applicable
	Solicited personal information	Applicable
Australian Privacy Principle 4—dealing with unsolicited personal information	Dealing with the receipt of PI without solicitation	Not Applicable
Australian Privacy Principle 5—notification of the collection of personal information	Reasaonable steps to notify individuals of PI collected	Partial Applicability
Australian Privacy Principle 6—use or disclosure of personal information	Use or disclosure	Not Applicable
	Written note of use or disclosure	Not Applicable
	Related bodies corporate	Applicable
	Exceptions	Not Applicable
Australian Privacy Principle 7—direct marketing	Direct marketing	Not Applicable
	Exceptions—personal information other than sensitive information	Not Applicable
	Exception—sensitive information	Not Applicable
	Individual may request not to receive direct marketing communications, etc.	Not Applicable
	Interaction with other legislation	Not Applicable
Australian Privacy Principle 8—cross-border disclosure of personal information	Disclosure of PI to overseas recipients	Not Applicable
Australian Privacy Principle 9—adoption, use, or disclosure of government-related identifiers	Adoption of government-related identifiers	Not Applicable
	Use or disclosure of government-related identifiers	Not Applicable
	Regulations about adoption, use, or disclosure	Not Applicable
Australian Privacy Principle 10—quality of personal information	PI collected is accurate and complete	Partial Applicability

Australian Privacy Principle 11—security of personal information	All	Applicable
Australian Privacy Principle 12—access to personal information	Access	Partial Applicability
	Exception to access—agency	Not Applicable
	Exception to access—organization	Partial Applicability
	Dealing with requests for access	Not Applicable
	Other means of access	Not Applicable
	Access charges	Not Applicable
	Refusal to give access	Not Applicable
Australian Privacy Principle 13—correction of personal information	Correction	Partial Applicability
	Notification of correction to third parties	Not Applicable
	Refusal to correct information	Not Applicable
	Request to associate a statement	Not Applicable
	Dealing with requests	Not Applicable

Appendix C Applicable Cybersecurity Regulations, Standards, and Guidelines

The table below is an exhaustive list of applicable regulations, standards, and guidelines grouped by sector or industry.

Sector/Audience	Name	Hyperlink
Banking and Finance	APRA CPG 235	http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk.pdf
Banking and Finance	PPG 234	http://www.apra.gov.au/crossindustry/documents/ppg_ppg234_msrit_012010_v7.pdf
Banking and Finance	ISO 27001/2	https://www.iso.org/isoiec-27001-information-security.html
Banking and Finance	COBIT 5	http://www.isaca.org/cobit/pages/default.aspx
General	NIST Cybersecurity Framework	https://www.nist.gov/cybersecurity-framework
General	Cybercrime Act 2001	https://www.legislation.gov.au/Details/C2004C01213
General	Risk Management of Enterprise Mobility Including Bring Your Own Device (BYOD)	https://www.asd.gov.au/publications/protect/enterprise_mobility_bring_your_own_device_byod.htm
General	Cyber Security for Contractors	https://www.asd.gov.au/publications/protect/Cyber_Security_for_Contractors.pdf
General	Privacy Amendment (Notifiable Data Breaches) Act 2017	https://www.legislation.gov.au/Details/C2016B00173
General and Government	Strategies to Mitigate Cyber Security Incidents	https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm
Government	Australian Government Protective Security Policy Framework (PSPF)	https://www.protectivesecurity.gov.au/Pages/default.aspx
Government	Information Security Manual (ISM)	https://www.asd.gov.au/infosec/ism/
Government	iRAP	https://www.asd.gov.au/infosec/irap.htm
Government and Healthcare	TGA	https://www.tga.gov.au/publication-issue/medical-devices-safety-update-volume-4-number-2-march-2016
Government	Information Security Management Guidelines: Risk Management of Outsourced ICT Arrangements (Including Cloud)	https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentInformationSecurityManagementGuidelines.pdf
Healthcare	Royal Australian College of General Practitioners (RACGP) Computer and Information Security Standards	https://www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/
Healthcare	National Health and Medical Research Council's "The Regulation of Health Information Privacy in Australia"	https://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/nh53.pdf
Healthcare	ISO 27001/2	https://www.iso.org/isoiec-27001-information-security.html
Healthcare	COBIT 5	http://www.isaca.org/cobit/pages/default.aspx
Insurance	Breach Notification	http://www.apra.gov.au/CrossIndustry/Pages/Breach-Notification.aspx
ISP	Telecommunications (Interception) and Listening Device Amendment Act	https://www.legislation.gov.au/Details/C2004C01072
ISP	Communications Alliance C650:2014 icode	http://www.commsalliance.com.au/__data/assets/pdf_file/0019/44632/C650_2014.pdf
ISP	Australian Communications and Media Authority's Australian Internet Security Initiative (ACMA, 2015)	https://www.cert.gov.au/aisi
ISP	ISO 27001/2	https://www.iso.org/isoiec-27001-information-security.html
ISP	COBIT 5	http://www.isaca.org/cobit/pages/default.aspx
Manufacturing	ISO 27001/2	https://www.iso.org/isoiec-27001-information-security.html
Manufacturing	COBIT 5	

Mining	ISO 27001/2	https://www.iso.org/isoiec-27001-information-security.html
Mining	ISO 27019	
Mining	COBIT 5	http://www.isaca.org/cobit/pages/default.aspx
NSW Government	Digital Information Security Policy	https://www.finance.nsw.gov.au/ict/priorities/managing-information-better-services/information-security
General	Privacy Act 1988	https://www.legislation.gov.au/Details/C2017C00283
General	Telecommunications Consumer Protection Code	http://www.commsalliance.com.au/Documents/all/codes/c628
General	Spam Act	https://www.legislation.gov.au/Details/C2014C00214
General	Do Not Call Register Act	https://www.legislation.gov.au/Details/C2015C00258
General	Payment Card Industry Data Security Standard	https://www.pcisecuritystandards.org/pci_security/standards_overview
General	Mobile Privacy—A Better Practice Guide for Mobile App Developers	https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers
General	Guide to Securing Personal Information	https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information
Telecommunications Providers	Telecommunications (Interception) and Listening Device Amendment Act	https://www.legislation.gov.au/Details/C2004C01072
Telecommunications Providers	Australian Communications and Media Authority's Australian Internet Security Initiative (ACMA, 2015)	https://www.cert.gov.au/aisi
Telecommunications Providers	ISO 27001/2	https://www.iso.org/isoiec-27001-information-security.html
Telecommunications Providers	COBIT 5	http://www.isaca.org/cobit/pages/default.aspx
Utilities	ISO 27001/2	https://www.iso.org/isoiec-27001-information-security.html
Utilities	ISO 27019	
Utilities	COBIT 5	http://www.isaca.org/cobit/pages/default.aspx
Utilities	NERC-CIP V5	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Appendix D Australian State Mobile Device Procurement Policies

The table below provides hyperlinks to relevant Australian state procurement policies for mobile devices. Note that some resources may not be mobile device specific but instead refer to general IT requirements.

State	Mobile Procurement Policy	Hyperlink
New South Wales	NSW Government Mobile Device and Application Framework	https://www.finance.nsw.gov.au/ict/sites/default/files/resources/NSW percent20Government20Mobile%20Device%20%20Application%20Framework.pdf
	General IT requirements protecting consumer data, security, and privacy	http://ec2-54-66-245-30.ap-southeast-2.compute.amazonaws.com/?q=node/194 http://beta32.procurepoint.nsw.gov.au/?q=node/239
Victoria	No specific policies found but previous mobile device security-related procurements exist through telecommunications contracts. Note that Microsoft O365 includes minimal EMM functionality.	http://www.procurement.vic.gov.au/State-Purchase-Contracts/Telecommunications-TPAMS2025-Services http://www.procurement.vic.gov.au/State-Purchase-Contracts/Microsoft-Enterprise-Agreement
Northern Territory	No mobile-specific policy found. Last IT procurement policy dated 2009.	https://nt.gov.au/industry/government/procurement-conditions-framework/conditions-contract/others/government-information-technology-contract
South Australia	No mobile-specific policy found.	
Queensland	No mobile-specific policy found, but "Departments should ensure that all legal and regulatory obligations under which they operate are observed when conducting procurement processes."	https://www.qgcio.qld.gov.au/documents/procurement-and-disposal-of-ict-products-and-services-implementation-guideline https://www.qgcio.qld.gov.au/documents/information-security-is18-information-standard
Tasmania	No mobile-specific policy found, but "Networking Tasmania protects the security, integrity and availability of your information assets through security practices based on industry standards, such as ISO 27001/. These supplier security practices are regularly audited and reviewed to ensure compliance with Government's requirements."	https://www.tmd.tas.gov.au/networking_tasmania/learn_about_networking_tasmania
Western Australia	The Department of Finance site recommends consideration of ASD Cloud Computing Security Considerations when assessing risk factors during procurement of cloud services.	https://www.finance.wa.gov.au/cms/Government_Procurement/Cloud_Computing/Cloud_Computing_Resources.aspx
Australian Capital Territory	No mobile-specific policy found.	

Appendix E Abbreviations and Acronyms

ABS	Australian Bureau of Statistics
ACMA	Australia Communications and Media Authority
ACSC	Australian Cyber Security Centre
APP	Australian Privacy Principles
ASD	Australian Signals Directorate
ATO	Australian Tax Office
AustCyber	Australian Cyber Security Growth Network
BYOD	bring your own device
COPE	company owned personally enabled
CVE	common vulnerabilities and exposures
FIPS	Federal Information Processing Standards
ICT	information and communication technology
IEC	International Electrotechnical Commission
IRAP	Information Security Registered Assessors Program
ISM	Information Security Manual
ISO	International Organization for Standardization
MDM	mobile device management
MTC	Mobile Threat Catalogue
NCCoE	National Cybersecurity Center of Excellence
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OAIC	Office of the Australian Information Commissioner
PSPF	Protective Security Policy Framework
SME	small and medium enterprise
SMS	short message service
VPN	virtual private network

Appendix F References

[1] G. Gilfillan. (2018, Feb 7). "Definitions and Data Sources for Small Business in Australia: a quick guide," Parliament of Australia. Available: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/Quick_Guides/Data.

[2] Financial System Inquiry. (2018, Jan 4). "Small- and Medium-Sized Enterprises." Available: http://fsi.gov.au/publications/interim-report/03-funding/small-med-enterprises/.

[3] Australian Government: Business. (2018, Jan 4). "Keep Your Business Safe from Cyber Threats," business.gov.au. Available: https://www.business.gov.au/info/run/cyber-security/keep-your-business-safe-from-cyber-threats.

[4] Australian Government. (2018, Jan 4). Stay Smart Online. Available: https://www.staysmartonline.gov.au/.

[5] Australian Government. (2018, Feb 1). "8129.0—Business Use of Information Technology, 2015-16," Australian Bureau of Statistics. Available: http://www.abs.gov.au/ausstats/abs@.nsf/mf/8129.0.

[6] Australian Government. (2014, Jan). "Report 1—Australian SMEs in the Digital Economy," Australian Communications and Media Authority. Available: https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Australian-SMEs-in-the-digital-economy-pdf.pdf?la=en.

[7] Australian Government. (2015, Mar). "Report 1—Australians' Digital Lives," Australian Communications and Media Authority. Available: https://www.acma.gov.au/~/media/Research%20and%20Analysis/Research/pdf/Australians%20digital%20livesFinal%20pdf.pdf.

[8] DeviceAtlas. (2018, Jan 4). "Web Usage of Device Names by Country." Available: https://deviceatlas.com/device-data/explorer/webusage-by-country/traffic/no-tablet/country/au/type/device_marketing.

[9] Android Open Source Project. (2018, Jan 4). "About the Android Open Source Project." Available: https://source.android.com/.

[10] Android Open Source Project. (2018, Jan 4). "Security Updates and Resources." Available: https://source.android.com/security/overview/updates-resources.

[11] L. Newman. (2017, Sept). "Inside Android Oreo's Quest to Protect Your Phone," WIRED. Available: https://www.wired.com/story/android-oreo-security-improvements/.

[12] *Mobile Threat Catalogue*, NIST NCCoE, 2018. Available: https://pages.nist.gov/mobile-threat-catalogue/.

[13] Australian Government. (2018, Feb). "Hacking," Australian Competition and Consumer Commission. Available: https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/hacking.

[14] Australian Government. (2018, Feb). "Phishing," Australian Competition and Consumer Commission. Available:

https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing.

[15] press-au@squareup.com. (2018, Jan 4). "Square Reader Now Sold in More Than 490 Retail Stores Across Australia, Through Officeworks, Apple and Bunnings," Square, Inc. Available: https://squareup.com/au/news/square-reader-now-sold-in-more-than-490-retail-stores-across-australia-through-officeworks-apple-and-bunnings.

[16] *Guide to Bluetooth Security,* NIST Special Publication 800-121 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, 2016. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-121/rev-2/draft/documents/sp800_121_r2_draft.pdf.

[17] Australian Government. (2018, Jan 4). "Small Business Entity Concessions," Australian Taxation Office. Available: https://www.ato.gov.au/business/small-business-entity-concessions/eligibility/.

[18] *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST Special Publication 800-124 Revision 1, 2013. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

[19] *Mobile Device Security—Cloud and Hybrid Builds Approach, Architecture, and Security Characteristics,* NIST Special Publication 1800-4, 2015. Available: https://nccoe.nist.gov/publication/1800-4b.

[20] Standards Australia. (2018, Feb 7). "What Is a Standard?" Available: http://www.standards.org.au/StandardsDevelopment/What_is_a_Standard/Pages/default.aspx.

[21] Australian Government. (2018, Jan 4). "Entities Covered by the NDB Scheme," Office of the Australian Information Commissioner. Available: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/entities-covered-by-the-ndb-scheme#small-business-operators.

[22] Australian Signals Directorate. (2018, Jan 4). *Essential Eight Explained,* Information Security Advice. Available: https://www.asd.gov.au/publications/protect/essential-eight-explained.htm.

[23] Australian Signals Directorate. (2018, Jan 4). "Cloud Computing Security for Tenants." Available: https://www.asd.gov.au/publications/protect/cloud-security-tenants.htm.

[24] Australian Government Information Security Manual. (2017). Australian Signals Directorate. Available: https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf.

[25] Australian Government. (2018, Jan 4). "Guide to Securing Personal Information," Office of the Australian Information Commissioner. Available: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

[26] Australian Government. (2018, Jan 4). "Mobile Privacy—A Better Practice Guide for Mobile App Developers," Office of the Australian Information Commissioner. Available: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-for-mobile-app-developers.

[27] W. Fabritius. (2017, April). “Assessment Report Microsoft Corporation Micrcosoft Azure,” bsi. Available: https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=498137f0-31da-4100-a323-35abf229b13b&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO%20Reports.
[28] Australian Government. (2018, Feb 7). Privacy Amendment (Notifiable Data Breaches) Act 2017, Federal Register of Legislation. Available: https://www.legislation.gov.au/Details/C2017A00012.
[29] Crowell Moring. (2018, Jan 4). “The Global Uptake of the NIST Cybersecurity Framework.” Available: https://www.crowell.com/files/20160215-The-Global-Uptake-of-the-NIST-Cybersecurity-Framework-Wolff-Lerner-Miller-Welling-Hoff.pdf.