Commissioner for Privacy and Data Protection

Victorian Information Security Network (VISN) Partners' Forum

14th December 2016

Questions & Answers

1	**How will this project interact/relate/reference the APP's of the Privacy Act (Cth.)?**

The Victorian Protective Data Security Standards (VPDSS) provides better practice outcomes for the protection of all public sector data held, generated or collected by or on behalf of Victorian Government organisations – this includes personal information as governed by "Part 3 – Information Privacy" of the Privacy and Data Protection Act 2014.

Victorian Information Privacy Principle (IPP) 4.1 – Data Security states, *"An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure"*.

These security requirements are similar to those set out in Commonwealth APP 11.1, *"An APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure"*

The Commissioner for Privacy and Data Protection regards that adherence to the VPDSS constitutes 'reasonable steps' under IPP 4.1. The office of CPDP has published further guidance on its website[1]

2	**Are you receiving any funding from the Treasury for your initiative?**

No additional funding has been allocated for this initiative to date.

3	**What are your procurement plans for this or next financial year?**

CPDP are working with government to identify opportunities and initiatives that will assist agencies or bodies understand and adhere to the Victorian Protective Data Security Framework (VPDSF). For example,

- systems that will assist agencies in the submissions of their Security Risk Profile Assessments and Protective Data Security Plans
- guidance material
- templates
- awareness training videos
- attendance at existing government forums
- creating new forums

4	**Will you help agencies secure budget to meet requirements?**

The VPDSF and guiding principles have been designed in a manner to assist and support organisations focus their efforts to their high-risk areas and manage their security programs within their existing budgets.

[1] https://www.cpdp.vic.gov.au/images/content/pdf/privacy_guidelines/IPP_4_Guidelines.pdf

The adoption of a risk-based approach consistent with the Victorian Government Risk Management Framework (VGRMF) is one of the fundamental principles of the VPDSF. A flexible approach to implementation of security measures provides your organisation with the autonomy to interpret your business needs and articulate your risk tolerance within your operating environment.

5 Why does Victoria have to have separate security standards? Why not adopt the Federal?

The main distinction between the VPDSF and the Protective Security Policy Framework (PSPF) is the scope of each framework. The VPDSF governs the protection of public sector data, whilst the PSPF governs the protection of all government assets.

The VPDSF and VPDSS are also the first of their kind to be legislatively mandated (Part 4 of the *Privacy and Data Protection Act (PDPA)*, 2014).

The VPDSS reflect the unique operating requirements of Victorian Government agencies or bodies, whilst supporting contemporary security standards both locally and internationally. Where appropriate, the controls for each standard reference existing Victorian Government policies, guidelines and procedures. This approach assists organisations leverage off existing effort previously undertaken to comply with existing Victorian Government requirements that will also meet security requirements. This approach should result in unnecessary duplication of effort.

To assist organisations in understanding the relationship of the VPDSS to the PSPF and other security standards, CPDP has mapped the requirements in a resource called the 'VPDSF Rosetta Stone'. Organisations applying the PSPF and other security standards will be able to easily assess their compliance against the VPDSS. This list will continue to expand and be updated over time[2].

6 Is this VPDSF different to frameworks designed in other states? And how does it compare?

The *Privacy and Data Protection Act 2014* (Vic) is the first of its kind - overseeing privacy, protective data security and law enforcement data security in a single Act. No other jurisdiction in Australia has a legislative framework compelling public sector organisations to adhere to a minimum set of security standards for the protection of official information.

Whilst drafting the VPDSF, CPDP comprehensively considered the PSPF requirements as well as other state and territory security frameworks to ensure consistency (where possible), whilst providing a Victorian environmental overlay. The Data Protection Branch actively supports and advocates interoperability of VPDSS with other states and territories frameworks. If any inconsistences are identified, we encourage feedback to the Data Protection Branch for consideration.

To assist organisations in understanding the relationship of the VPDSS to other security standards, CPDP has mapped the requirements in a resource called the 'VPDSF Rosetta Stone'. Organisations applying other security standards will be able to easily assess their compliance against the VPDSS. This list will continue to expand and be updated over time[3].

7 Will you address a common requirement to store consumer data on shore only?

[2] https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20170119_VPDSF_Rosetta_Stone_V2.0.pdf

[3] ibid

The VPDSS does not prevent offshoring of public sector data. Each Victorian Government organisation should determine the best storage options for their needs based on their own risk assessment.

CPDP advises agencies to follow the five step action plan, and consider and legal /regulatory requirements applicable to that organisation.

8 Can you elaborate how the standards apply to critical infrastructure services?

The VPDSS does not replace or supersede any regulatory requirements on critical infrastructure providers to manage the security of their systems and information. If any inconsistences are identified, we encourage feedback to the Data Protection Branch for consideration.

9 Are you considering People-Centric Security (PCS) as additional risk mitigation?

Gartner describes People-Centric Security (PCS) as a framework that provides personal autonomy in how they use information and devices, and the level of security they chose to adopt when using it[4]. It places an emphasis on "individual accountability and trust, and de-emphasizes restrictive, preventative security controls."[5] "A key prerequisite for PCS is the ability and context for individual users to make the appropriate risk-based decisions…"[6].

The guiding principles of the VPDSF are designed to enable organisations to evaluate their current and prospective security practices, including establishing a positive security culture and utilising a risk management approach. It offers a balanced view of ensuring all stakeholders are aware of their responsibilities, but also positions the organisations to make informed decisions on what security measures are appropriate to help achieve its business objectives.

VPDSF guiding principle two states that "risk management empowers an organisation to make informed decisions and prioritise security efforts."[7] Principle four emphasises a positive security culture, under which "clear personal accountability and a mature understanding of managing risk, responsibility and reputation allows an organisation to function effectively and support the delivery of government services"[8] A natural outcome of these two principles working hand in hand will:

- "see personnel thinking and acting in more security-conscious ways
- help reduce organisations' protective data security risks
- enable the secure delivery of government services."[9]

These principles, in conjunction with the VPDSS align with the basic premise of PCS, but compel organisations to consider their risk posture when selecting what security controls should be implemented and applied. In turn, organisations are empowered to ensure investment in these controls are appropriate and tailored to reflect their business needs and resources.

To ensure greater benefit from this approach, organisations are encouraged to reach out and consult with all stakeholders to help identify security risks. The outcomes of this approach will create a more agile

[4] https://www.gartner.com/webinar/2976918

[5] https://www.gartner.com/webinar/2976918

[6] http://www.gartner.com/smarterwithgartner/lessons-in-how-to-implement-people-centric-security/

[7] https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20160628%20VPDSF%20Framework%20June%202016%20v1.0.pdf

[8] ibid

[9] ibid

business-operating model and will help establish a security culture where individuals recognise their responsibilities and understand the role they play. This is consistent with PCS principles.

10 Is there a plan to extend the collaboration with other groups including physical security (PHYSEC)?

The inaugural VISN forums sought to gain insight into, and understand the needs of stakeholders both across VPS and with partner groups. This includes collaborating with other groups on topics across each of the protective security domains, of which physical security is captured. A VPS physical security group has previously been established in the Data Protection GovDex community and included in the consultation on the development of the standards

11 How do you plan to manage and lessen the push back to your strategy from ICT and PHYSEC?

The VPDSF requires security practitioners to have a thorough understanding of their broader business context; it's information assets, risks and resources available to them to help protect public sector data.

CPDP plans to work with the relevant practitioner groups to ensure consistent messaging.

Organisations should consider all aspects of protective security when implementing controls to protect their information to ensure the best outcome with limited resources. The VPDSF should complement and build on existing ICT and PHYSEC controls for the security of information needed to do business.

If any inconsistences are identified, we encourage feedback to the Data Protection Branch for consideration.

12 Does the VPDSS apply to long-term retention - i.e. VERS record keeping as defined by PROV?

The VPDSS applies to public sector data across its lifecycle – i.e. from creation through to disposal. Disposal can include transfer to or archival with another organisation, or destruction conducted in accordance with PROV standards.

The security controls for information will depend on the confidentiality, integrity and availability. These requirements may change over time as the value of the information changes.

13 Should we give you the HR and Corporate Services / FMO contacts within our organisations?

Practitioners are encouraged to join the Data Protection GovDex community by emailing security@cpdp.vic.gov.au with a request to join.

CPDP will continue to develop targeted guidance to assist organisations apply the VPDSF based on needs identified by organisations. To better enable this, CPDP may work with existing practitioner forums or develop sub-groups of the VISN based on function.

14 How will you be applying pressure on CEO's to drive practical change? Cultural change is one part, but what else?

The VPDSF has been developed to assist the CEO achieve his or her business objectives by supporting a risk based approach to security. VPDSF guiding principle six states "Sound protective data security practices enable an organisation to achieve its business objectives in an efficient, effective and economic manner." This principle alone should drive an Agency Head or CEO to adopt the VPDSF.

Additionally there are legislative and reputational considerations Agency Head or CEO may wish to consider. Part 4, s89 (5) of the PDPA (2014) requires the public sector body Head for each agency or body to submit a copy of their organisation's Protective Data Security Plan (PDSP) to CPDP. CPDP will use these plans to support the monitoring and assurance function of the office and gather a view of protective data security practices across the Victorian government. This view will be presented to the Victorian parliament through the tabling of the CPDP annual report. In addition, CPDP will conduct assurance assessments of agencies or bodies using the outputs of the SRPA, PDSP and agency annual reporting to drive the annual assessment calendar.

It is anticipated through the culmination of these activities, e.g. driving a positive security culture across the Victorian government and the reporting and review cycles, these will influence CEO's to see great value in building security capability aligned to the VPDSF and VPDSS.

15 How will you embed the approach within the governance structures across Victorian Government and/or within individual organisations?

Protocol one across most of the VPDSS requires executive sponsorship of security practices within their organisations. CPDP encourages organisations to embed security across all areas of their organisation[10]

CPDP will continue to engage with VPS at all levels not just practitioner and executive level to ensure all stakeholders hear the messages

16 It's important to have standards but without legislation how will you reinforce change in the culture?

The VPDSS and VPDSF are mandated by legislation – the Privacy and Data Protection Act (2014). In saying that, legislation does not immediately translate to a change in culture. Instead, cultural change will require a transformation program extending across the VPS.

VPDSF guiding principle four acknowledges this and highlights the importance of developing a strong security culture *"organisational culture is underpinned by the attitudes and behaviours of personnel and, in particular, their shared values and beliefs that interact with the organisation's structures and control systems to produce behavioural norms… The VPDSF seeks to establish security as a natural element of organisational culture…. where protective data security practices are reflected in everyday business operations and all personnel take a shared responsibility. By embedding security in organisational culture, it becomes something that 'is', rather than something an organisation 'has' or 'does'."*[11]

To support organisations, CPDP will continue to produce a range of guides and tools to support a transformation in security attitudes and behaviours.

17 How do the agencies responses to the standards contribute to the CPDP sharing instruments in your Act?

The sharing instruments set out in the PDPA (2014) address more than just data security, with information sharing references regarding personal information included in Part 3 of the Act - i.e.

- Temporary Public Interest Determinations (TPIDs) and Public Interest Determinations (PIDs)

[10] https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20160601_Embedding_security_into_your_organisation_V1.013.pdf

[11] https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20160628%20VPDSF%20Framework%20June%202016%20v1.0.pdf

that permit a departure from selected IPPs

- Information Usage Arrangements (IUAs) where agencies seek modification from an IPP
- Certifications, where a particular privacy practice or program is endorsed.

Under these each of these mechanisms, the Commissioner assesses the proposal to determine whether the suggested practices or program are in the public interest.

Note: Organisations cannot seek to a PID or TPID for Information Privacy Principle 4 - Data Security or IPP 6 - Access and Correction.

By implementing the VPDSS, agencies will be addressing Information Privacy Principle 4.1 requiring organisations to take reasonable steps to protect personal information.

18 Cyber security is a matter of national security, does VPDSF add to the current *Australian Cyber Security Strategy*, which is on a national level?

The Australian Cyber Security Strategy provides a forward focus and identifies objectives to manage cyber threats to the nation.

It is worth noting that the Victorian Cyber Security Strategy is currently being developed which is expected to complement the Australian Cyber Security Strategy and support the VPDSF.

The VPDSF complements and supports both cyber security strategies. If any inconsistences are identified, we encourage feedback to the Data Protection Branch for consideration.

19 Should there be a 6th step in the action plan about the ability to respond/recover when there is a breach or problem?

Step 5 of the VPDSF Five Step Action Plan relates to managing risks across the information lifecycle. CPDP see response/recovery as a natural component of managing risks across the information lifecycle.

20 Will there be any guidance on how to identify risks after information value has been assessed. List of generic risks or threats, etc.?

Yes, VPDSS Standard 2 – Security Risk Management provides guidance material that will assist organisations identify risk.

In addition to this, CPDP is currently working on a number of initiatives and projects to support security risk management. This includes technical and non-technical guidance material, and will be made available soon.

21 How will agencies keep up with the risk dimension - especially with regards to ICT security - constantly evolving and one days position is very different to the next day

Security risk management is an ongoing and iterative process. The requirements for organisations to deliver biennial SRPA and PDSP deliverables will provide CPDP visibility of their security risk landscape.

To help businesses stay across evolving ICT threats, organisations should subscribe and engage with teams and groups such as Computer Emergency Response Teams (CERTs) e.g. AusCERT or CERT Australia, who

have access to up-to-date threat information. The Australian Signals Directorate and Australian Cyber Security Centre also provide advice on mitigating ICT threats.

22 You say these Standards don't apply to public health services. Define the extent of this please. How about funded agencies that are not public health organisations but still registered under the Health Act?

Part 4, s84 (2) (a) of the PDPA (2014) sets out the applicability of the VPDSF / VPDSS, identifying which organisations are in and out of scope.

Under this section of the Act, certain public health services (i.e. public hospitals, ambulance service, etc.) are listed as being exempt from the provisions of Part 4. As such these exempt organisations are not expected to submit reports to CPDP on their level of adherence to the VPDSS.

Instead, public health organisations need to be cognisant of their existing security obligations under other sections of the PDPA (2014) and related legislation.

The Information Privacy Principles (IPPs) and in particular IPP4, draws a nexus between organisations responsibility for protecting personal information and the VPDSS. Information Privacy Principle (IPP) 4.1 requires organisations to 'take reasonable steps to protect the personal information they hold from misuse, loss, and unauthorised access, modification or disclosure'.

As such, organisations may have an indirect obligation in applying the VPDSS in ensuring that they take reasonable steps to protect personal information. The measures that are necessary to protect personal information will differ depending on a number of factors, such as the type of information in question, the value of that information, and the potential consequences if an individual's privacy were compromised. Depending on the types of information you are dealing with, there may be other legal and regulatory obligations that need to be considered. It is up to the organisation to understand what types of information they are dealing with and any obligations that accompany this.

Indirect obligations may also stem from Standard 9 of the VPDSS, which directs 'in-scope' agencies or bodies to "ensure that contacted service providers with access to public sector data, do not do an act or engage in a practice that contravenes the Victorian Protective Data Security Standards (VPDSS)"[12]. As such, these VPS agencies or bodies may call on public health service organisations to offer them a level of assurance around their security practices.

These 'assurance requests' may take different forms, as each VPS organisation may require something different. Ultimately public health organisations need to be able to demonstrate to their VPS partners that the security practices of their organisation offer the proper degree of protection to the information they are sharing.

CPDP encourage organisations to seek legal advice if they have any doubts about their obligations under the Act.

23 Is the VPDSF derived from the Federal Government's Information Security Manual (ISM) / International Standard ISO 27001?

The VPDSF is the overall scheme for managing protective data security risks in Victoria's public sector. It consists of:

[12] https://www.cpdp.vic.gov.au/images/content/pdf/data_security/VPDSS%20Standards%20v1.1%20Jul2016.pdf

- the Victorian Protective Data Security Standards (VPDSS)
- the Assurance Model
- supplementary security guides and supporting resources.

The VPDSS assist government operations by ensuring the right people have access to the right information at the right time. They are based on national (e.g. PSPF/ISM) and international (e.g. AS/ISO 27001) security policies and practices. They also recognise the Victorian public sector's unique operating requirements and diverse range of agencies and bodies.

To assist organisations, CPDP has developed a resource titled the 'VPDSF Rosetta Stone'. The Rosetta maps each of the VPDSS to existing protective security standards and guides. This resource includes a 'core' and 'supplementary' section. The core includes more common security reference material that Victorian public sector agencies and bodies have operated under in the past. The 'supplementary' section maps other material that organisations may use such as:

- Australian Signals Directorate (ASD) - Information Security Manual (ISM) 2016
- Information Security Forum (ISF) - Good Practice Standard for Information Security 2016
- ISO27002:2015
- Payment Card Industry - Data Security Standards (PCI - DSS)

Join our GovDex community, watch our website and download the CPDP Mobile App to stay abreast of updates to our guidance material.

24 How would you like to engage with the private sector to support this initiative?

CPDP would like industry to contact CPDP when they are developing their own products or conduct forums to help government organisations implement the VPDSF. This will allow CPDP to ensure consistency of messaging.

Other industry partners who are provided with, collect or generate information on behalf of an organisation will also need to provide assurance to the VPS agency or body that their information is managed securely.

25 Is there a VICGOV Yammer group for VISN?

Not yet, but we are exploring this as a communication channel to support our existing engagement tools.

26 Can we get the slides via email? Sli.do didn't deliver

It was unfortunate that we had technical difficulties just prior and within the first five minutes of the forum that kept us from uploading the PowerPoint presentation.

The slides for both the VPS and Partner sessions are available on the CPDP website[13]

[13] https://www.cpdp.vic.gov.au/menu-data-security/data-security-community-events/visn-summary-slides

Comments & Responses

1	**Love the video it's really clear and aligned.**
	The video provides a general overview of the VPDSF and a high level introduction into the VPDSS. Individual organisations will still need to consider their specific risks/security measures in any training and awareness programs they deliver, but are welcome to access our video[14] Industry should speak with CPDP prior to development of products to ensure that your products are aligned with CPDP messaging.
2	**First time I've heard from VPS as a funded agency.**
	CPDP is working hard to reach out to all the partners of Victorian Government organisations, including funded agencies, to improve information security across Victoria. We understand the vital services that funded agencies provide to Victorian Government and the vast amounts of Victorian public sector data that you collect and hold as a result of these services. As mentioned there is an expectation from in-scope VPS organisations that provide you with official (including personal) information that the VPDSS will be applied to that information. Any new contracts or Memorandums of Understanding should reflect this expectation.
3	**The NDIS has already trumped any State privacy arrangements with regards to health information**
	The NDIS along with any other legislative requirements take precedence over any VPDSF controls if they conflict. The VPDSF complements and supports legislative requirements. If any inconsistences are identified, we encourage feedback to the Data Protection Branch for consideration.
4	**It would be useful to show diagrammatically how the frameworks, policies, controls (technical & non-technical) apply. All are needed and should not be seen to have different values compared to each other. Resistance is often not [deliberate] - it is an inability to move forward due to a lack of clarity.**
	Part Two of the VPDSF document[15] sets out the framework structure and hierarchy in Figure 1 (pictured below).

[14] https://www.cpdp.vic.gov.au/images/videos/data-security/CPDP-Revisions-FINAL-HV%201.0%20D.mp4

[15] https://www.cpdp.vic.gov.au/images/content/pdf/data_security/20160628%20VPDSF%20Framework%20June%202016%20v1.0.pdf

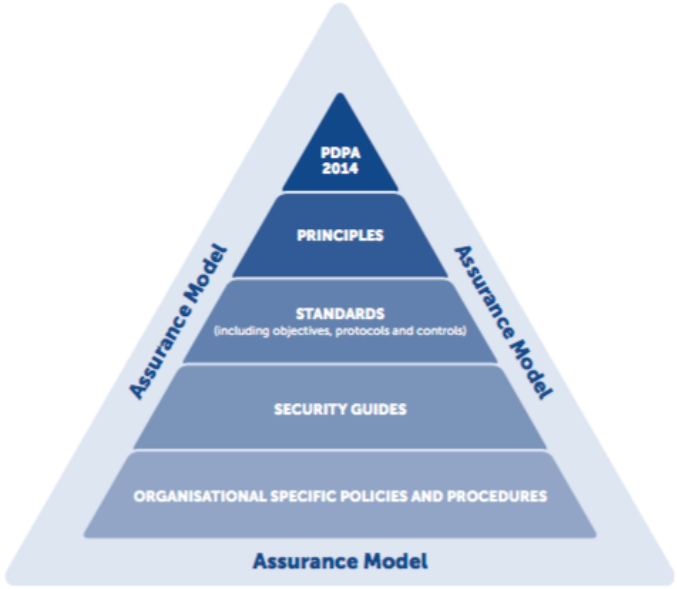

Figure 1. VPDSF structure

A description of each tier and supporting descriptions are also provided in this section.

If organisations are unclear on how any of the material relates to other components of the VPDSF, we encourage you to email security@cpdp.vic.gov.au with any questions.

5 Great stuff. Well done!

DPB want to thank all who attended and participated in the first VISN Partners Forum!