SUBMISSION - WV TECHNOLOGIES

2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY DISCUSSION PAPER

WV Technologies commends the Australian Government and the Expert Advisory Board for its vision and progress towards making Australia the most cyber secure nation by 2030. We are pleased to provide this submission and advice as experts in the ICT disposals/decommissioning industry.

The correct and safe disposals of end-of-life ICT equipment is, in our experience, usually not provided sufficient attention by organisations from every sector. While organisations often work hard to implement measures to protect the front door, they are giving away the keys to the back door through improper ICT disposals on a scale this is difficult to comprehend.

Ensuring correct ICT disposals is closing the loop in the information chain and protecting employee's data, client's data, corporate IP, national security and citizens data. The protection of this data through proper ICT disposals should be the responsibility of any organisation which holds it, and these organisations should be provided clear instructions from Government on how to do this.

See a report published by Price Waterhouse Coopers (which also features our organisation as industry experts) March 2023 and which outlines the issues and risks which we support.

https://www.pwc.com.au/cyber-security-digital-trust/critical-infrastructure/critical-infrastructure-ewaste-data-security-threat.html

We can be contacted to provide further information on a confidential basis; however a summary of the key issues is provided here:

1. In our 5 years sampling experience, we have found that around one in every 250 devices from Government and industry at its end-of-life is making its way into the used IT market internationally with sensitive/security classified data intact. These data bearing assets are being exported globally at scale, including to countries such as China, Pakistan and the UAE. Or equipment is being sold on the local market, able to be accessed by Australian criminal organisations. The cost of this scale of data leakage to the community is unknown.

2. On a single HDD found on an online marketplace the quantity of sensitive files, if printed and stacked, would reach the height of the Sydney Tower. Factor this across the tens of thousands of data bearing media being leaked annually, the scale is hard to comprehend.

3. Organisations believe that ICT disposals is a simple process and just a matter of wiping hard drives. However, many other data containing/storage devices exist in modern ICT equipment.

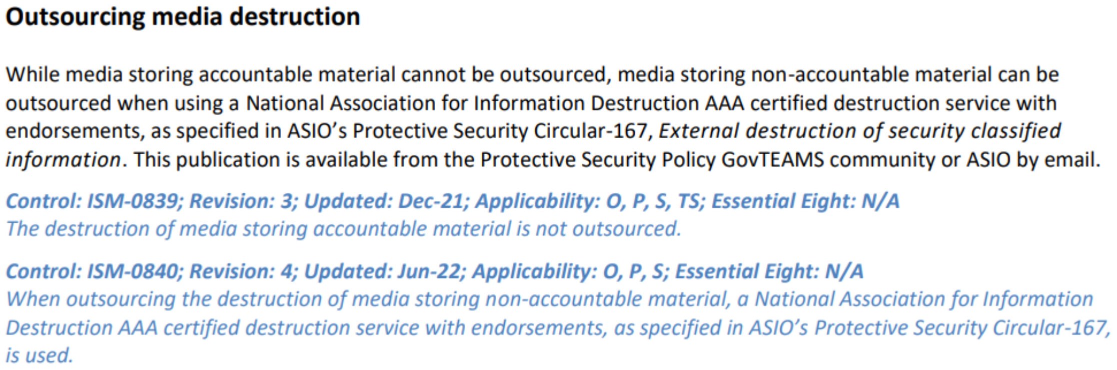
4. Many organisations complete ICT sanitisation using internal staff, uncertified suppliers or rely on auction houses to complete this vital task. There is limited certification of this process.

5. We do not believe there is any organisation in Australia that has a register of all data bearing media devices in their organisation, let alone their supply chain. If they don’t know what media bearing devices they have, then how can they be sure they have all been sanitised/destroyed at end-of-life?

6. The majority of organisations do not use suppliers that are independently audited for data sanitisation/destruction processes. This means they are not following the recommendations of the Australian Privacy Principles, Chapter 11, which recommends following the Information Security Manual (ISM). The ISM Security Control 0840 mandates the use of a NAID AAA certified supplier with PSPF Endorsements for media destruction.

7. Despite ISM security control 0840 stating that a NAID AAA certified supplier must be used, many Government tenders released and awarded do not include this requirement.

   See below from the Information Security Manual Page 81



Outsourcing media destruction

While media storing accountable material cannot be outsourced, media storing non-accountable material can be outsourced when using a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's Protective Security Circular-167, *External destruction of security classified information*. This publication is available from the Protective Security Policy GovTEAMS community or ASIO by email.

Control: ISM-0839; Revision: 3; Updated: Dec-21; Applicability: O, P, S, TS; Essential Eight: N/A
The destruction of media storing accountable material is not outsourced.

Control: ISM-0840; Revision: 4; Updated: Jun-22; Applicability: O, P, S; Essential Eight: N/A
When outsourcing the destruction of media storing non-accountable material, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's Protective Security Circular-167, is used.

8. The regulatory framework is fragmented, confusing and non-descriptive. The Information Security Manual has a strong set of security controls; however this document does not appear to be enforceable as policy. The OAIC and the Australian Privacy Principles do not provide direct advice on what to do with redundant ICT equipment and the principle of "taking reasonable steps" is seemingly invoked. The Protective Security Policy Framework does not mandate the ISM or provide clear guidance that any organisation which holds Government data, via contracts or other correspondence, must also follow the PSPF and ISM. The result is that large corporates, including in high security supply chains, do not have clear instructions on what to do with end-of-life ICT equipment, and essentially self-regulate.

9. Clear guidance is not provided on what is the equivalent classification for non-government corporate data (i.e. a Green, Amber, Red system or one that matches the Government system of Official, Official Sensitive, Protected, Secret, Top Secret could be used).

KEY RECOMMENDATIONS

In order to effectively mitigate the risks inherent in ICT disposals, we recommend the following:

- The ISM is mandated under the PSPF for all Government and any organisation which deals with Government. Further, that the Australian Privacy Principles and the OAIC provide clear guidance on what to do with redundant ICT equipment, with the most likely solution being to mandate adherence to the ISM for media sanitisation and destruction.
- The ISM Control 0840 is updated to include media sanitisation as well as destruction.
- NAID AAA certification and the audit process be reviewed with industry experts so that the certification is increasingly robust and in line with modern changes in technology and the Australian regulatory frameworks and threat landscape.
- All organisations should be required to keep a register of all data bearing media and data bearing devices, this could over time also extend to their supply chain if they are at certain tiers.

CYBER SECURITY STRATEGY DISCUSSION PAPER QUESTIONS WITH DIRECT RESPONSE

1. *What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030 and*

Please see above where we outline the case for more focus on proper ICT disposals.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

Please see above where we outline that the Information Security Manual provides strong controls for the ICT disposal process, and it could be mandated across industry and Government as a strong first step. This could be via existing frameworks the PSPF for Government and contracting corporate organisation and via the OAID and the Australian Privacy Act 1988 and APPs for industry and the Critical Infrastructure Act or via the new proposed Cyber Security Act.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

Many areas of Commonwealth Government are not following the ISM and PSPF as they regularly release and award tenders with no mention of the NAID AAA certification. Many Departments continue to use suppliers which do not have the certification which is clearly outlined as a requirement in the ISM.

Commonwealth Departments do not properly report when data security incidents are notified to them which reduces the opportunity for learnings. WV Technologies has notified many Departments of data leaked and to our knowledge they have not reported this in any of the obligatory reporting mechanisms.

Commonwealth Government Departments usually have incomplete asset registers, storerooms full of data bearing obsolete equipment, and no register of data bearing media in the organisation and whether it has been destroyed, sanitised or lost. Each device has multiple data bearing media (HDD/SSD, SD Card, Optical, EEPROM chips, BIOS, SIM, Network Cards, Remote Access Cards, Cache Cards etc.) and a register of these should be maintained so that risk can be evaluated. Over time, this register should extend into supply chains so that contracting organisations are also held accountable for proper disposal of data bearing media.

WV Technologies can provide further advice on systems for making this possible if required.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Clear concise directions on what responsibilities all organisations have to dispose of end-of-life ICT equipment. Then the market can provide the solutions.

17. How should we approach future proofing for cyber security technologies out to 2030?

For ICT Disposals, the ISM should firstly be mandated, and then also be regularly updated as it is, but with additional consultation with Industry so that the latest technologies and strategies to address risk can be included in the security controls.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

For ICT Disposals, the ISM should firstly be mandated, and then also be regularly updated as it is, but with additional consultation with Industry so that the latest technologies and strategies to address risk can be included in the security controls.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Organisations should have a register of all data bearing media and devices in their organisation and then be held responsible for the status of them e.g. in use, sanitised/destroyed or missing. Over time, this should be extended to the supply chains so that risk points can be identified and suppliers evaluated for their cyber security control.

WV Technologies thanks the Department and the Advisory Board for the opportunity to provide this submission and advice in our area of unique industry expertise, ICT disposals.

Our team is available to provide further comments if required.