Appendix A:
Submissions and comments

We have consulted with all agencies and we considered their views when reaching our audit conclusions. As required by the *Audit Act 1994*, we gave a draft copy of this report, or relevant extracts, to those agencies and asked for their submissions and comments.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the relevant agency head.

Responses received

Response provided by the Chair, Cenitex

Level 9, 35 Collins Street ,
Melbourne, Victoria, 3000
(PO Box 2750)
ABN 56 375 109 796

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
31/35 Collins Street
Melbourne VIC 3000

Reference Number: 3490925

14/10/2025

Dear Mr Greaves

Re: Proposed report, the Cybersecurity of IT Servers

Thank you for your letter dated 1 October 2025 providing the *Proposed report, the Cybersecurity of IT Servers* for my consideration and comment.

I have considered the report, and I support the recommendations that align to Cenitex.

Cenitex has over the recent horizon taken significant investment to uplift and modernize the security, hosting and asset management of Cenitex and customer products.

Security is a key pillar of Cenitex services, and we continue to implement and refresh security services specifically tailored to the needs of government entities.

Cenitex's current strategy and deployment of servers to the cloud environment is significantly reducing the cyber security threat in the Cenitex environment.

Cenitex as the State Government's shared service provider, has a key role to play in the Cybersecurity of its own assets and as a provider of cybersecurity services to our customers. The continued challenge that is faced by Cenitex and its customers is to balance prudent investment with the ever-changing nature of cybersecurity along with the broad range of IT investment required.

I am pleased to provide the Cenitex action plan that outlines how Cenitex will implement the recommendations.

OFFICIAL: Sensitive

I would like to take the opportunity to thank your team for their professional engagement with Cenitex.

Should you or your team require any further information or assistance please contact Paul Kruspe Director Transformation on [redacted] or by email [redacted].

Yours sincerely,

[redacted]

Rodd Cunico

Chair

cc. Adrian Carbone, Acting Chief Executive Officer

cc. Paul Kruspe Director, Transformation and Strategic Programs

cenitex

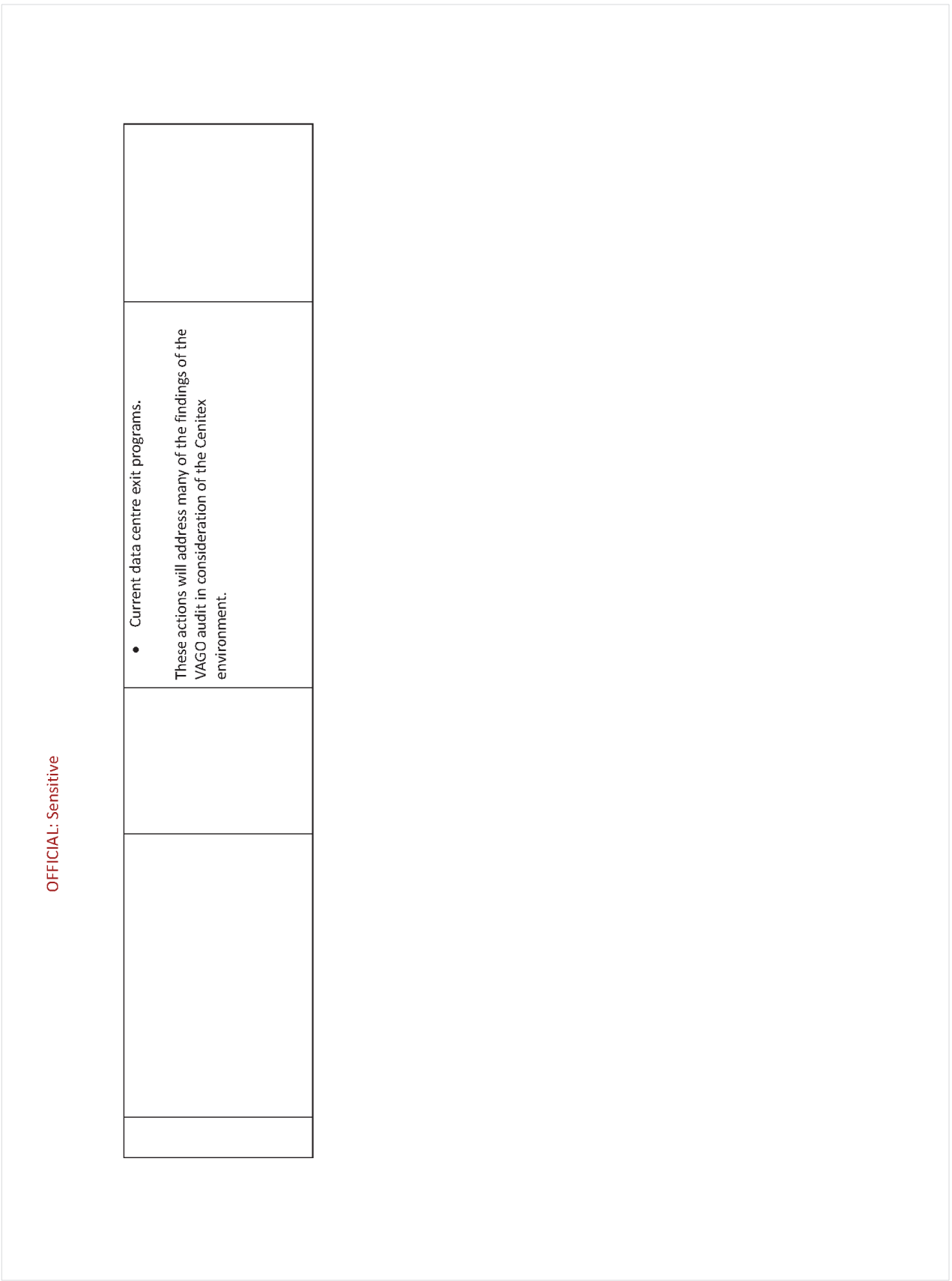
VICTORIA State Government

Cenitex action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date

1	Improve their tracking of all IT servers by (where necessary):
	• using automated asset discovery tools
	• establishing and maintaining a centralised IT server asset register using appropriate server tracking software
	• assigning clear responsibility for the accuracy and completeness of IT server inventory.
		☒ Yes
		☐ No
		☐ In part
		☐ In principle
			Cenitex has in place all of the VAGO recommendations.
			
			This includes:
			• The use of multiple automated asset discovery tools
			• A central source asset register utilising contemporary server tracking software.
			• A robust governance process including:
			  ○ Asset register Health Metrics, which automatically run and report on a daily assessment of the completeness of the Server records.
			  ○ Focused process governance including a Data Quality Working Group & CMDB Working Group.
			In addition, the current program to exit the legacy Data centres will continue to increase the level of server compliance and increased cloud asset visibility.
				Completed

2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	Cenitex will reduce its on-premises servers as workloads are migrated under the strategic Multi-Cloud program and continue to prioritise its existing security compliance initiatives that will further strengthen security controls. Specifically, these will be addressed as part of in progress initiatives: • The Security Compliance program, • Scheduled operating system upgrades	December 2027


OFFICIAL: Sensitive
• Current data centre exit programs.
These actions will address many of the findings of the VAGO audit in consideration of the Cenitex environment.

Response provided by the Secretary, Department of Education

Department of Education

Secretary

2 Treasury Place
East Melbourne Victoria 3002
Telephone +61 3 9637 2000

COR25170857

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
[redacted]

Dear Mr Greaves

Proposed report on Cybersecurity of IT servers

Thank you for your letter of 1 October 2025 and the opportunity to comment on the proposed report for this audit. The department is committed to implementing and maintaining cybersecurity measures to protect its IT servers from threats.

The department has reviewed the proposed report, and an action plan to address the 2 recommendations applicable to the department is attached.

Should your staff wish to discuss the department's response, please contact Shamiso Mtenje, Executive Director, Integrity, Assurance and Executive Services Division on [redacted] or [redacted].

Yours sincerely

[redacted]

Tony Bates PSM
Secretary
15/10/2025

Encl.: DE's action plan

DE Final action plan: Cybersecurity of IT servers (with action owners)

#	Recommendations: That DE:	Response	#	The Department will:	By:
1	Improve their tracking of all IT servers, where necessary, by: • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	Accept	1.1	Enhance the use of discovery and server and cloud management tools to extend automated asset discovery across on-premise and cloud-based environments.	Sep 2027
			1.2	Establish and maintain a federated technology asset register governed under a technology asset management framework.	Dec 2026
			1.3	Implement a formal accountability framework for inventory and lifecycle management under a technology asset management framework.	Dec 2025
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter for the department. • implementing improvements consistent with the plan.	Accept	2.1	Develop an action plan to improve technical security controls applied to servers, informed by the findings identified in the management letter.	Dec 2025
			2.2	Implement the actions as per the action plan and due dates to address the findings noted in the management letter.	Dec 2027

Response provided by the Secretary, Department of Energy, Environment and Climate Action

Department of Energy, Environment and Climate Action

PO Box 500, East Melbourne,
Victoria 8002 Australia

SEC-251000030

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31 35 Collins Street
Melbourne Victoria 3000

Via email: [redacted]

Dear Auditor-General

Proposed draft report – Cybersecurity of IT Servers

Thank you for your letter of 1 October 2025, inviting comment on your office's proposed draft report for the performance engagement: *Cybersecurity of IT Servers,* received 1 October 2025.

The Department of Energy, Environment and Climate Action (DEECA) recognises the need to effectively protect our IT servers from threats.

I can advise that DEECA accepts recommendation one outlined in the proposed draft report and accepts in-principle, recommendation 2 as this will be subject to DEECA's resource capacity. A proposed action plan for addressing these recommendations is enclosed.

I thank your staff for their work and look forward to a continued productive relationship with your office.

Yours sincerely

[redacted]

Kate Houghton PSM
Secretary

10 / 10 / 2025

Encl.

VICTORIA State Government

Official - Sensitive

Department of Energy, Environment and Climate Action – action plan to address recommendations from VAGO's report: *Cybersecurity of IT Servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ **Yes** ☐ **No** ☐ **In part** ☐ **In principle**	1. DEECA will develop a policy that assigns clear responsibilities where all IT server owners are required to maintain accuracy and completeness of the centralised DEECA IT server register utilising existing IT server tracking software.	26 June 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☐ **Yes** ☐ **No** ☐ **In part** ☒ **In principle**	1. DEECA will develop a plan to improve its technical security controls applied to IT servers, as identified within the management letter. This will be based on the department's risk control priorities and resource capacity. 2. DEECA will develop a schedule for implementing the improvement plan for technical security controls applied to IT servers.	31 July 2026 30 October 2026

VICTORIA State Government | Energy, Environment and Climate Action

Response provided by the Secretary, Department of Families, Fairness and Housing

Secretary

Department of Families, Fairness and Housing

50 Lonsdale Street
Melbourne Victoria 3000
Telephone: 1300 475 170
GPO Box 1774
Melbourne Victoria 3001
www.dffh.vic.gov.au

VAGO File No: 34909 25

DFFH File No: BAC-CO-59183

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Via email: [redacted]

Dear Mr Greaves

Thank you for providing the proposed report for VAGO's Cybersecurity of IT servers performance audit.

The Department of Families Fairness and Housing welcomes this report and supports the audit's findings, acknowledging the importance of cybersecurity and the protection of information held by the department.

The department has reviewed the proposed report and the two recommendations directed at all agencies. The department accepts in principle Recommendation 1 and accepts Recommendation 2, noting that implementation will involve working with the department's third-party vendors, and will be contingent on identifying funding.

I would like to take this opportunity to thank your staff for working collaboratively with the Department of Families, Fairness and Housing.

Yours sincerely

[redacted]

Peta McCammon
Secretary

16/10/2025

Encl.

DFFH action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • **a)** using automated asset discovery tools • **b)** establishing and maintaining a centralised IT server asset register using appropriate server tracking software • **c)** assigning clear responsibility for the accuracy and completeness of IT server inventory.	☐ Yes ☐ No ☐ In part ☒ In principle	**a)** The department accepts the recommendation to use automated asset discovery tools. The department will work with our third-party vendors to enhance its tracking of IT servers. **b)** The department accepts in principle the establishment and maintenance of a centralised IT server asset register using appropriate server tracking software. Implementation is contingent on identifying funding. **c)** The department accepts the assignment of clear responsibility for maintaining an accurate and complete inventory of IT servers and will implement as a priority	**a)** 30 June 2026 **b)** 31 October 2026 **c)** 31 October 2025
2	Strengthen technical security controls by: • **a)** developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • **b)** implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	**a)** The department accepts this recommendation to develop a plan to improve technical security controls. Work is underway to identify server security risks, with a formal roadmap planned to prioritise mitigation from high to low risk. **b)** The department accepts this recommendation; Implementation of a plan will be contingent on identifying funding	**a)** 30 June 2026 **b)** 30 June 2027

Response provided by the Secretary, Department of Government Services

Department of Government Services

Level 5
1 Macarthur Street
East Melbourne Victoria 3002
Telephone: (03) 9651 5111
dgs.vic.gov.au

Our ref: BSEC-250900155

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

By email: [redacted]

Dear Auditor-General

VAGO PROPOSED REPORT: CYBERSECURITY OF IT SERVERS PERFORMANCE AUDIT

Thank you for your letter dated 1 October 2025 enclosing the proposed report *Cybersecurity of IT Servers* for consideration and comment.

The Department of Government Services (DGS) acknowledges the report and accepts its findings. DGS is committed to continually improving its technical security controls and implementing the recommendations made by VAGO for DGS and its customer departments, including the Departments of Premier and Cabinet and Treasury and Finance.

I have enclosed a copy of DGS' action plan responding to the audit recommendations.

If your office requires further information, please have them contact Dovid Clarke, Chief Information Security Officer, DGS at [redacted].

Yours sincerely

[redacted]

Jo de Morton
Secretary

15 / 10 /2025

Enc DGS action plan to address recommendations in Cybersecurity of IT servers

DGS action plan to address recommendations in *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ Yes ☐ No ☐ In part ☐ In principle	Progressive deployment of automated asset discovery tools across the IT server environment to capture and reconcile all operating systems and applications that aligns with IT Asset Management Policy guidance. This work has already commenced.	31 December 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Develop remediation plans for all servers running on legacy operating systems. Undertake a security review of legacy servers with the aim of protecting servers with layered security. 2. Implement improvement plans, informed by findings contained in the VAGO Management Letter, to address weaknesses in platform-specific technical security controls and departmental cyber security controls. 3. Collaborate with Cenitex and third-party vendors to implement technical security controls that meet whole-of-government minimum requirements (that will be determined in response to recommendation 3).	1. 31 December 2026 2. 30 June 2027 3. 31 December 2027
3	In consultation with relevant agencies, DGS should issue guidance to agencies that establishes requirements for: • effective tracking of server inventory • applying and maintaining technical security controls for servers • reviewing and testing the effectiveness of technical security controls • managing servers with operating systems that no longer receive mainstream support.	☒ Yes ☐ No ☐ In part ☐ In principle	DGS will develop whole-of-government guidance for the minimum requirements for technical security controls for all Victorian Government agencies.	30 June 2026

Response provided by the Secretary, Department of Health

Secretary

Department of Health

50 Lonsdale Street
Melbourne Victoria 3000
Telephone: 1300 650 172
GPO Box 4057
Melbourne Victoria 3001
www.health.vic.gov.au
DX 210081

VAGO File No: 34909 25

DH File No: BAC-CO-59186

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Via email: [redacted]

Dear Mr Greaves

Thank you for providing the proposed report for VAGO's *Cybersecurity of IT servers* performance audit.

The Department of Health welcomes this report and supports the audit's findings, acknowledging the importance of cybersecurity and the protection of information held by the department and Victoria's health system.

The department has reviewed the proposed report and the two recommendations directed at all agencies. The department accepts in principle recommendation 1 and accepts recommendation 2, noting that implementation will involve working with the department's third-party vendors, and will be contingent on identifying funding.

I would like to take this opportunity to thank your staff for working with the Department of Health on this important audit.

Yours sincerely

[redacted]

Jenny Atta PSM
Secretary
15/10/2025

Attachment 1- DH Recommendation Action Plan - VAGO *Cybersecurity of IT servers*

DH action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • **a)** using automated asset discovery tools • **b)** establishing and maintaining a centralised IT server asset register using appropriate server tracking software • **c)** assigning clear responsibility for the accuracy and completeness of IT server inventory.	☐ Yes ☐ No ☐ In part ☒ In principle	**DH** **a)** The department accepts the recommendation to use automated asset discovery tools. The department will work with its third-party vendors to enhance tracking of the department's IT servers. **b)** The department accepts in principle the recommendation for the establishment and maintenance of a centralised IT server asset register using appropriate server tracking software. Implementation is contingent on identifying funding. **c)** The department accepts the assignment of clear responsibility for maintaining an accurate and complete inventory of IT servers and will implement this action as a priority.	**DH** **a)** 30 June 2026 **b)** 31 October 2026 **c)** 31 October 2025
			HTS **a)** The department accepts in principle the recommendation to use automated asset discovery tools and has already partly implemented this. Full implementation is contingent on identifying funding. **b)** The department accepts in principle the establishment and maintenance of a centralised IT server asset register using appropriate server tracking software. Implementation is contingent on identifying funding. **c)** HTS currently has clear responsibilities in this area.	**HTS** **a)** 31 December 2028 **b)** 31 December 2028 **c)** Complete

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
2	Strengthen technical security controls by: • **a)** developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • **b)** implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	**DH** **a)** The department accepts this recommendation to develop a plan to improve technical security controls. Work is underway to identify server security risks, with a formal roadmap planned to prioritise mitigation from high to low risk. **b)** The department accepts this recommendation. Implementation will be contingent on identifying funding	**DH** **a)** 30 June 2026 **b)** 30 June 2027
			HTS **a)** The department accepts this recommendation and will develop a plan as a priority. **b)** The department accepts this recommendation. Implementation of a plan will be contingent on implementing recommendations 1a and 1b and identifying funding.	**HTS** **a)** 31 December 2025 **b)** 31 December 2028

Response provided by the Secretary, Department of Jobs, Skills, Industry and Regions

OFFICIAL

Department of Jobs, Skills, Industry and Regions

GPO Box 4509
Melbourne ,Victoria 3001 Australia
Telephone: +61 3 9651 9999

Ref: CSEC-2-25-27264

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VICTORIA 3000

Dear Mr Greaves

CYBERSECURITY OF IT SERVERS PROPOSED REPORT

Thank you for your letter dated 1 October 2025 on the Cyber Security of IT Servers reasonable assurance performance audit.

The Department of Jobs, Skills, Industry and Regions (the department) acknowledges the proposed report and findings. Whilst the department does not agree with all the assessments made, the department remains committed to strengthening its cybersecurity posture and implementing the relevant recommendations.

Feedback on the management letter and the department's action plans to address the recommendations are provided as attachments to this correspondence.

If you require further information, your team can contact Karan Gill, Chief Audit Officer on [redacted] or [redacted].

Yours sincerely

[redacted]

Matt Carrick
Secretary

15/10/2025

VICTORIA State Government

DJSIR action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☐ Yes ☐ No ☐ In part ☒ In principle	DJSIR accepts this recommendation in principle and will undertake a detailed review of these controls as part of its Cyber Strategy. This will include assessment and identifying how each can be addressed either through current capability or funding for the uplift of these automated services. The assessment will be undertaken for DJSIR managed cloud platforms and not those hosted by Cenitex.	June 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☐ Yes ☐ No ☐ In part ☒ In principle	DJSIR accepts this recommendation in principle as it currently apply several industry controls including NIST, Essential 8 and VDPSS. The CIS Benchmark is another series of controls that can be applied where there may be gaps in the management of servers. DJSIR will undertake an assessment of the CIS Benchmark to identify opportunities to uplift our security framework for cloud systems including: • enforcing time-bound access for privileged actions • processes or policies relating to hardened images. Identified opportunities will be implemented in 2026-27 subject to implementation funding.	June 2026 for assessment June 2027 for implementation

Response provided by the Secretary, Department of Justice and Community Safety

Department of Justice and Community Safety

Secretary

Level 26
121 Exhibition Street
Melbourne Victoria 3000
Telephone: (03) 8684 0501
justice.vic.gov.au

Our ref: EBC 25092918

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Via email: [redacted]

Proposed report: Cybersecurity of IT servers

Dear Mr Greaves

Thank you for your letter of 1 October 2025 providing the proposed report and management letter for your audit on Cybersecurity of IT servers.

The department is committed to improving how it manages controls to mitigate the risk of cybersecurity incidents and threats.

Please see the attached action plan for addressing the 2 recommendations for all departments.

If you have any questions or require further information, please contact Julianne Brennan, Executive Director, Governance and Assurance on [redacted] or via email at [redacted].

Yours sincerely

[redacted]

Emma Cassar
Secretary

20/10/2025

DJCS action plan

Cybersecurity of IT servers

#	VAGO recommends that all agencies:	Response	#	DJCS will:	By:
1	Improve their tracking of all IT servers (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	Accept	1	Improve tracking of all DJCS IT servers by: • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	30-Jun-27
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	Accept	2	• Use a risk-based approach to develop a plan to address the key/high-risk security control weaknesses. • Execute the plan to remediate those weaknesses.	30-Jun-27

Response provided by the Secretary, Department of Premier and Cabinet

Department of
Premier and Cabinet

1 Treasury Place
Melbourne, Victoria 3002 Australia
Telephone: 03 9651 5111
dpc.vic.gov.au

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

BSEC-250900432

By email: [redacted]

Dear Auditor-General

Thank you for your letter dated 1 October 2025 enclosing the proposed report *Cybersecurity of IT Servers* for consideration and comment.

The Department of Premier and Cabinet (DPC) acknowledges the report and accepts its findings. DPC is committed to continually improving our technical security controls and implementing the recommendations from VAGO. We are working with the Department of Government Services (DGS), our shared services provider, to address the recommendations.

I have enclosed a copy of DGS' action plan prepared by DGS in response to the recommendations of the audit.

Should your office require further information, they may contact Dovid Clarke, Chief Information Security Officer, DGS at [redacted]

Yours sincerely

[redacted]

Jeremi Moule
Secretary

15 / 10 / 2025

Encl.

VICTORIA State Government

DGS action plan to address recommendations from *Cybersecurity of IT servers* for DPC, DTF and DGS

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Deploy asset discovery tools across the IT server environment to capture and reconcile all operating systems and applications that align with internal IT Asset Management Policy guidance.	1. 31 December 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Develop remediation plans for all servers running on legacy operating systems; and undertake a security review of legacy servers with the aim of protecting servers with layered security. 2. Implement improvement plans, informed by findings contained in the VAGO Management Letter, to address weaknesses in platform-specific technical security controls and departmental cyber security controls. 3. Collaborate with Cenitex and third-party vendors to implement technical security controls that meet WOVG minimum requirements.	1. 31 December 2026 2. 30 June 2027 3. 31 December 2027

Response provided by the Secretary, Department of Transport and Planning

Department of Transport and Planning

GPO Box 2392
Melbourne, Victoria 3001 Australia

Ref: BSEC-1-25-4326

Mr Andrew Greaves
Auditor-General of Victoria
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000
E: [redacted]

Dear Mr Greaves

Victorian Auditor-General's Office - Cybersecurity of IT servers - Proposed report

Thank you for your letter of 1 October 2025 inviting the Department of Transport and Planning (the Department) to respond to the *Cybersecurity of IT servers* proposed report (the Report).

The Department manages cyber risks in accordance with Victorian Government standards, policy and processes. On behalf of the Department, I acknowledge the Report's findings that there are opportunities to strengthen how agencies track their server environments and to improve the maturity of technical security controls for servers examined in this audit.

The Department has made significant investment in its Trusted and Secure program which is designed to mature the Department's cyber environment. Initiatives continue to be added or evolved as the cyber landscape continuously changes and gaps in our maturity are identified.

The Department accepts both of the Report's recommendations in principle and has prepared an action plan which is enclosed with this letter.

Thank you for the opportunity to comment on the Report.

[redacted]
Jeroen Weimar
Secretary

Date: 15 October 2025

Enc: DTP action plan - Cybersecurity of IT servers

DTP action plan

Cybersecurity of IT servers

The Department of Transport and Planning (DTP) action plan to address the recommendations from *Cybersecurity of IT servers*:

No	VAGO recommendation	DTP response	Due date
1	All agencies to improve their tracking of all IT servers by (where necessary): – Using automated asset discovery tools – Establishing and maintaining a centralised IT server asset register using appropriate server tracking software – Assigning clear responsibility for the accuracy and completeness of IT server inventory.	**Accepted in principle** The Department of Transport and Planning (DTP) will improve tracking of all IT servers hosted in an enterprise datacentre or IaaS environment by: – Using native asset discovery tools for cloud platforms. – Establishing and maintaining a centralised IT server asset register consolidating all hosting environments. – Assigning clear responsibility for the accuracy and completeness of IT server inventory.	31 March 2027
2	All agencies to strengthen technical security controls by: – Developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency – Implementing improvements consistent with the plan.	**Accepted in principle** DTP will strengthen technical security controls for servers hosted in an enterprise datacentre or IaaS environment by: – Developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter. – Implementing improvements consistent with the plan.	31 March 2027

Response provided by the Secretary, Department of Treasury and Finance

Department of Treasury and Finance

1 Treasury Place
Melbourne Victoria 3002 Australia
Telephone: +61 3 9651 5111
dtf.vic.gov.au

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

BORG-250900534

By email: [redacted]

Dear Auditor-General

VAGO PROPOSED REPORT: CYBERSECURITY OF IT SERVERS PERFORMANCE AUDIT

Thank you for your letter dated 1 October 2025 enclosing the proposed report *Cybersecurity of IT Servers* for consideration and comment.

The Department of Treasury and Finance (DTF) acknowledges the report and accepts its findings. DTF is committed to continually improving its technical security controls and implementing the recommendations from VAGO. We are working with the Department of Government Services (DGS), our shared services provider, to address the recommendations.

I have enclosed a copy of DTF's action plan prepared by DGS in response to the recommendations of the audit.

Should your office require further information, they may contact Dovid Clarke, Chief Information Security Officer at [redacted]

Yours sincerely

[redacted]

Chris Barrett
Secretary

15/10/2025

Encl.

OFFICIAL

DGS action plan to address recommendations from *Cybersecurity of IT servers* for DTF

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ Yes ☐ No ☐ In part ☐ In principle	Progressively deploy automated asset discovery tools across the IT server environment to capture and reconcile all operating systems and applications that aligns with internal IT Asset Management Policy guidance.	31-December-2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Develop remediation plans for all servers running on legacy operating systems. Undertake a security review of legacy servers with the aim of protecting servers with layered security. 2. Implement improvement plans, informed by findings contained in the VAGO management letter, to address weaknesses in platform-specific technical security controls and departmental cyber security controls 3. Collaborate with Cenitex and third-party vendors to implement technical security controls that meet WOVG minimum requirements	1. 30-June-2026 2. 30-June-2027 3. 31-December-2027