ORANGA TAMARIKI
Ministry for Children

OIA-CE-2025-02845

11 April 2025

s9(2)(a)
[redacted]

Tēnā koe s9(2)(a)

Thank you for your email, received on 19 March 2025, to Oranga Tamariki—Ministry for Children (Oranga Tamariki) requesting further information on the selection process for security and access control solutions. Your request has been considered under the Official Information Act 1982 (the Act).

I have responded to each part of your request below.

1. *Was the selected supplier licensed under the PSPPIA 2010 at the time of their submission and negotiation for security services with Oranga Tamariki?*

2. *Were the employees of the selected supplier licensed under the PSPPIA 2010 at the time of the submission, consultation, and negotiation for security services with Oranga Tamariki?*

The preferred vendor complied with applicable licensing requirements under the Private Security Personnel and Private Investigators Act 2010 (the PSPPIA) when they submitted their RFP response, including by having a subcontractor holding licences under the PSPPIA at the time of the RFP response.

While Oranga Tamariki has completed initial phases of the procurement process and selected a preferred vendor, it is now in the due-diligence and negotiation phase. The finalisation of the contract will be subject to completion of several activities. These activities include security risk assessments, and reviewing necessary licensing and certifications, among other things.

Oranga Tamariki understands all relevant personnel held the applicable certifications required under the PSPPIA at the time of the RFP response. As noted above, the negotiation phase is ongoing.

3. *Can you please provide a copy of the RfP for CCTV and Access Control Services?*

The Registrations of Interest (ROI) documents are available on the Government Electronic Tender Service (GETS). As provided in the ROI documents, the shortlisted vendors were invited to submit a Response for Proposal (RFP). The RFP was therefore provided to the shortlisted vendors only.

Please find attached as Appendix One a copy of the RFP document.

4. *Was the selected solution(s) tested and / or approved for use by the NZSIS Physec teams and meet the requirements outlined in the NZISM?*

Oranga Tamariki works closely with the NZSIS on the implementation of various government-mandated security framework documents, including NZISM. The NZSIS has advised that it is the responsibility of Oranga Tamariki responsibility to conduct proper due-diligence activities by following its security policies and conducting any necessary risk assessments internally.

5. *Was Rule 44 of the Government Procurement Rules considered during the procurement for security services?*

Oranga Tamariki adheres to all of the Government Procurement Rules and follows the Government Chief Digital Officer (GCDO) frameworks. Additionally, it follows the Certification and Accreditation (C&A) framework in the NZISM for security assessments when assessing vendors or products.

6. *(a) Was a formal threat, vulnerability and risk assessment completed, as outlined in the Protective Security Requirements guidance, on the selected supplier / solution, and*

Please refer to the response to question 1. In addition, Oranga Tamariki performs comprehensive certification and accreditation activities for both security and privacy, utilising external independent security providers to assess and mitigate risks before any system is deployed live in our environment.

(b) Does OT believe the decision adheres to the Governments Cloud Computing Strategy of keeping government data in NZL where possible?

Oranga Tamariki adheres to GCDO's applicable guidance, advice and strategies. Oranga Tamariki also complies with various frameworks and common capabilities, including the adoption of public Cloud services. Additionally, Oranga Tamariki ensures compliance with the C&A framework in the NZISM for security assessments when assessing vendors or products.

7. *Did Oranga Tamariki contact the Government Chief Digital Officer (GCDO) for advice and / or guidance?*

Oranga Tamariki did not need to contact the GCDO specifically as it already adheres to GCDO's guidance and advice, including the ICT strategy for government.

8. *Are digital images, by way of still or video, of children within the care of Oranga Tamariki considered Confidential by the NZ Govt. classification system?*

Oranga Tamariki holds various data classified up to the level of Sensitive / Restricted. As such, no data held by Oranga Tamariki is considered Confidential.

9. *In your response, you made the following statement, "The preferred supplier is responsible for the technologies used for the solution.". Does having the solution provider select the technology treatments meet the Five Principals of Govt. Procurement? Were the Government Procurement Charter points applied during the procurement process?*

To clarify, our statement in the response to the previous response refers to the fact that the preferred vendor is responsible for the implementation and support of technologies used for the solutions. However, Oranga Tamariki is responsible for the assessment and selection of technologies as part of the solutions.

Oranga Tamariki may make the information contained in this letter available to the public by publishing this on our website with your personal details removed.

I trust you find this information useful. Should you have any concerns with this response, I would encourage you to raise them with Oranga Tamariki. Alternatively, you are advised of your right to also raise any concerns with the Office of the Ombudsman. Information about this is available at www.ombudsman.parliament.nz or by contacting them on 0800 802 602.

Nāku noa, nā

Nick Lane
Head of Health Safety and Security
People Culture and Enabling Services

SECTION 1

RFP released: 20/11/2024

Deadline for RFPs: 4 pm 12 December 2024

Offer Validity Period: 6 months

Oranga Tamariki – Ministry for Children

https://www.orangatamariki.govt.nz

Request for Proposal: Implementation and Support of Closed Circuit Television (CCTV) and Electronic Access Control (EAC) Solutions

1. This opportunity in a nutshell

This procurement is for Respondents to assist Oranga Tamariki – Ministry for Children in the implementation and support of its Closed Circuit Television (CCTV) and Electronic Access Control (EAC) solutions for Youth Justice as well as Care & Protection Residences. The same solution may be leveraged for other Oranga Tamariki office sites/work environments.

Oranga Tamariki currently operates secure Care and Protection residences and Youth Justice residences at seven physical locations in New Zealand both in the North and South islands and around the major cities. These will be henceforth collectively referred to as Residences in this document.

Here are the 7 Residences:

- Korowai Manaaki, Wiri, Auckland
- Whakatakapokai, Weymouth, Auckland
- Te Maioha o Parekarangi, Rotorua
- Te Au rere a te Tonga, Palmerston North
- Te Puna Wai o Tuhinapo, Christchurch
- Epuni, Lower Hutt
- Puketai, Dunedin

There are also 81 staff sites (Commercial) and 163 Homes requiring CCTV & EAC Services.

For purposes of this RFP the deployment will be described in three Tranches; Deployment of the Residences will be Tranche 1, for the Commercial Sites Tranche 2, and then finally the Homes Tranche 3.

2. Detailed Requirements

2.1 CCTV Requirements

Oranga Tamariki wishes to appoint a suitably qualified and accredited CCTV supplier that meet the following requirements:

1. End-to-end integrated CCTV solution that is scalable, accessible from anywhere and provides insights and information
    - Modern CCTV cameras
    - Compliant with government security standards
    - Connected to telecommunications network via Oranga Tamariki provided zero trust network.
    - Connected to site operations room or similar, and centralised national operations centre
    - Backend management servers - Cloud-based or effective and secure localised options. (Note: Oranga Tamariki's strategy is cloud-first and currently has a presence in AWS, Azure

Cloud platforms).

2. Cameras plus associated hardware and licensing
    - Specifications for Indoor & outdoor cameras.
        - High Definition Resolution and image quality
        - Surveillance coverage and field of view (e.g. Wide Angle lenses)
        - Dome, Bullet, 360, Fish-eye, PTZ and multi head camera options
        - Low light and Night vision (spotlight with high lumen capability)
        - Scalability
    - Waterproof and vandal proof where required.
    - Wired mainly for power, data, and control.
    - Ability to record video and audio (including privacy shield for audio).
    - Spot Monitors (and NVR / decoders if required)
    - SD Cards (note any locally stored images must also be backed up to the cloud)
    - Camera housing and other hardware (for example servers, disks etc.)
    - Any other on-premises hardware (for example UPS for backup)
    - Any routers and switching equipment if required
    - Any firmware and updates/upgrades required
    - Any specific requirements or corrections to lighting to ensure optimal operation of CCTV
    - On site CCTV notices/signs conforming with the Privacy Act 2020
    - Any other equipment required e.g. cabinets, brackets, fastenings, associated cabling and conduit.

3. Operating/Control System for the cameras, software, and hardware
    - Local and centralised solutions for operator control.
    - System update/upgrade and patch processes.
    - Monitoring solution to support effective and efficient real-time monitoring of footage by kaimahi.
    - Motion detection and smart analytics
    - Real-time alerts
    - Managed integration with other physical security controls (EAC, RT)
    - Search and retrieval (rapid recall to find cameras of interest ad find events images)
    - Features to preserve evidence to the standards required for presentation in a court of law
    - Privileged access control and audit logging.
    - Ability to view a live site map with detailed components of cameras/devices on site

4. Network
    - Solution working on zero trust network
    - Compliant to required encryption standards
    - Buffering/fail-over solution for video footage during network outage
    - Specify required networking WAN and LAN components (e.g. circuit, router, switch hub)

5. Design and implementation plan

a) Design approach
· Standards-based design.
· A design methodology for camera placement.
· Camera/system selection based on standards, placement requirements, monitoring, and overall system design.
b) Pilot site
· Deploy to one commercial site to test concept/system
· Review and confirm approach
c) POC residence site
· Deploy to one residence site to test concept/system
· Review and confirm approach
d) Deploy to Remaining (6) secure residences [Tranche 1 Sites]
· Deploy, then test and sign off
e) Deploy to 81 corporate sites [Tranche 2 Sites]
· For each site Design & Plan, Deploy, then test and sign off
f) Deploy to 163 homes [Tranche 3 Sites]
· Deploy to one Home site to test design
· Review and confirm approach
· For each site Design & Plan, Deploy, then test and sign off
·
g) Training
· Initial training of all staff on the new access control
· Train the trainer and provision of online training resources for authorised staff on the new systems

6. Logistics and maintenance
   - NZ based sparing/repair and logistics centre.
   - In country spares/stock available to replace all key items for 1 residence
   - Field workforce to maintain all site equipment available 24/7.
   - Commitment to onsite response and restoration times at all sites with trained CCTV and EAC staff

7. Data Storage and Retrieval
   - Options around Cloud-based storage or effective and secure localised storage option. (Note: Oranga Tamariki's strategy is cloud-first and currently has a presence in AWS, Azure Cloud platforms).
   - Local remote storage for backup only if cloud-based storage is utilised.
   - Cost-effective storage archiving options.
   - Ability to securely and efficiently access and share footage (both internally within the Ministry

and externally with partner agencies such as Police).

- Ability to view, retrieve and archive footage.
- All user access to footage is restricted to approved users and user-accesses logged and auditable.

8. Management, Remote System Monitoring and Support services 24/7
    - Support for each component by the supplier, Service desk, Technical support, and OEM support.
    - System software and hardware patching and management/delivery of any firmware/software updates and upgrades
    - 24/7 Monitored alerts and on call support
    - Account management team during business hours
    - System based alerting and monitoring system of components for faults and maintenance.
    - Knowledge based articles
    - Inbuilt asset management as part of monitoring system.
    - Contribute to the design of new site requirements or site changes
    - Ongoing input into operational processes and training requirements

2.2 EAC Requirements

1. End-to-end electronic Access System plus associated hardware and licensing
    - Modern EAC hardware and componentry
    - Compliant with government security standards
    - Connected to telecommunications network via Oranga Tamariki provided zero trust network.
    - Connected to site operations room or similar, and centralised national operations centre
    - Backend management servers - Cloud-based or effective and secure localised options. (Note: Oranga Tamariki's strategy is cloud-first and currently has a presence in AWS, Azure Cloud platforms).

2. Electronic Access System Component specifications
    - Electronic Locks e.g. electromagnetic clamp mortice
    - Proximity Card Readers
    - Terminal Pin-pads
    - Alarm Terminals
    - Access cards and fobs
    - Door Controllers
    - Door position monitoring reed switches
    - Exit Devices and emergency egress devices
    - Intruder detection PIRs (e.g. Glass breaks and 360)
    - Duress buttons, pendants and mimic panels
    - Duress Strobe and Piezzo

- Operator's workstations
- UPS back up
- Security signage
- Other door hardware such as vandal resistant bezels, auditable alarms (standard on fail to secure), cabling, 3-stage heavy duty closers, hold-backs, handles

3. Operating/Control System software and firmware for the Access Controllers and associated hardware, including Cloud platforms
    - Local and national systems for management.
    - Included Software System support update, upgrades, and patch processes.
    - Monitoring solution to support effective and efficient real-time monitoring of access by kaimahi.
    - Privileged access control and audit logging.
    - Fire release must be included on all electronically locked doors on fire and emergency egress paths
    - Ability to integrate with building management system
    - Ability to integrate with Connected to CCTV camera system to provide a single dashboard/console (Refer Oranga Tamariki ROI for CCTV released on GETS on 20th May 2024).
    - Ability to integrate with other communication devices at sites, mobiles, R7 radios, and Body cameras (in the future).
    - Ability to integrate with Oranga Tamariki's Level 1 IT Service Desk
    - Connected to site components via Oranga Tamariki provided zero trust network.
    - Connected to Azure Active Directory.

4. Additional EAC features
    - We know that modern EAC systems have a number of advanced features. We want to implement basic and core features in the initial phases so that current risks are mitigated. A further phase will implement the remaining features.
    - Additional features in an EAC system beyond core access control we are interested in are – Monitoring, Visitor management, Room and Intruder alarms, Duress alarms, Secure Key management, Intercom and Locker management.

5. Network
    - Solution working on zero trust network
    - Compliant to required encryption standards
    - Specify required networking WAN and LAN components (e.g. circuit, router, switch hub)

6. Design and implementation plan

a) Design approach
· Standards-based design.
· A design methodology for electronic access control system and intruder detection including door hardware schedules.
· Device /system selection based on standards, requirements, monitoring, and overall system design.

b) Pilot site
· Deploy to one commercial site to test concept/system
· Review and confirm approach
c) POC residence site
· Deploy to one residence site to test concept/system
· Review and confirm approach
d) Deploy to Remaining (6) secure residences [Tranche 1 Sites]
· Deploy, then test and sign off
e) Deploy to 81 corporate sites [tranche 2 Sites]
· For each site Design & Plan, Deploy, then test and sign off
f) Deploy to 163 homes [tranche 3 Sites]
· Deploy to one Home site to test design
· Review and confirm approach
· For each site Design & Plan, Deploy, then test and sign off
·
g) Training
· Initial training of all staff on the new access control
· Train the trainer and provision of online training resources for authorised staff on the new systems

7. Logistics and maintenance capability
   - NZ based sparing/repair and logistics centre.
   - In country spares/stock available to replace all key items for 1 Secure residence
   - Field workforce to maintain all site equipment available 24/7.
   - Commitment to onsite response times all sites with trained EAC staff
   - Proactive maintenance and evergreen asset refresh process
8. Data Storage and Retrieval
   - Cloud-based storage (Note: Oranga Tamariki's strategy is cloud-first and currently has a presence in AWS, Azure Cloud platforms).
   - Cost-effective storage archiving options.
   - Ability to view, retrieve and archive records.
   - All user access to records is restricted to approved users and user-accesses logged and auditable.

9. Management, Remote System Monitoring and Support services 24/7
   - Support for each component by the supplier, Service desk, Technical support, and OEM support.
   - System software and hardware patching and management/delivery of any firmware/software updates and upgrades
   - 24/7 Monitored alerts and on call support
   - System based alerting and monitoring system of components for faults and maintenance.

- Knowledge based articles
- Inbuilt asset management as part of monitoring system.
- Contribute to the design of new site requirements or site changes
- Ongoing input into operational processes and training requirements

3. Integration

The operating security management systems should fully integrate both the CCTV and EAC systems and components and have ability to manage all within the one system.

All the principal parts of the CCTV and EAC systems must be supportive of and compatible with each other. This includes but is not limited to cameras, switches, controllers, electronic door hardware, communications devices, cabling, interfaces, software, power supplies, related hardware, power supplies, and any other related equipment.

4. Emergency Response Requirements

4.1 In the event of a major emergency (an emergency is the result a natural disaster or intentional damage due to Tamariki at site which results in critical health , safety and security issues requiring immediate attention) at any of the sites, an immediate supplier emergency response team will be required to manage and implement the supplier's services more specifically to

- Project manage the supplier's response, participate in Incident Management Team meetings with Oranga Tamariki Key staff.
- Supplier team experience must be, suitably qualified senior technicians with Oranga Tamariki facility experience and clearance.
- Regular reporting, updates as required
- Evidencing with documents and photos for insurance claims
- assess damage and required ,
- Provide initial replacements work arounds
- Redesign if required
- replace/repair and restore all damaged equipment
- Confirm test and sign off with Oranga Tamariki Incident Management Team leads
- restore site to normal operations, post all rectification

Also, a commitment dispatch the onsite maintenance resources immediately to site and stand up a project team to respond immediately on request from Oranga Tamariki.

Note the Target restoration is Live up and running with 24 hours for Critical CCTV cameras

5. Costing

5.1 The detailed implementation and support costing:

Response: Costs to be detailed in the attached spreadsheet: CCTV&EAC Costing template

6. Service Levels Required

6.1 Please provide Prioritisation definitions and performance target levels:

Table 1

Prioritisation	Support Hours	Response Time The elapsed time between call rec	Status Update Frequency of updates to Oranga Tamariki on the status service Restoration	Resolution Time (return to operation) The elapsed time between the notification of the Incidents and confirmation back to Oranga Tamariki that service has been restored	Service Credit Amount	Performance Target
	24/7 x 7 days	15 mins	30 mins	2 hours	TBC	- [100%] of Incident tickets are responded to within the Response Times. - [100%] of Incident tickets are resolved within the Resolution Time.
Priority 2	24/7 x 7 days	30 mins	60 mins	4 hours	TBC	- [100%] of Incident tickets are responded to within the Response Times. - [100%] of Incident tickets are resolved within the Resolution Time.
Priority 3	Business Hours	2 business hours	4 business hours	1 business day	TBC	- [90%] of Incident tickets are responded to within the Response Times. - [90%] of Incident tickets are resolved within the Resolution Time.
Priority 4	Business Hours	4 business hours	8 business hours	3 business days	TBC	- [90%] of Incident tickets are responded to within the Response Time. - [90%] of Incident tickets are resolved within the Resolution Time

6.2 Response to be detailed in the format as per the Table 1

7. Contract term

Oranga Tamariki anticipate that the Contract will commence on 01 March 2025 with an implementation of Trance 1 Sites taking approximately 6 months. Then a Contract term post trance 1 implementation is:

Description	Years
Initial term of the Contract	3 years

8. Other tender documents

In addition to this RFP that outlines the procurement, we refer you to the following documents. These documents are included in the RFP pack and form part of this RFP:

- The Response Form to fill out your response: *CCTV & EAC RFP Response Form*
- Oranga Tamariki's Master Services Agreement: *Master Services Agreement Template – August 2024*
- Oranga Tamariki's standard statement of work template for support services: *Support SoW CCTV & EAC 1.11.24*
- Appendices to the support SoW: *Template Appendices to SOW – CCTV and EAC Support Services*
- Oranga Tamariki's standard implementation template: *Design & Install Statement of Work*
- CCTV&EAC Costing template [EXCEL Spreadsheet]

Submitting your RFP

a. Submit your RFP by email/electronically to the following address: Procurement_TechandChannels@ot.govt.nz
b. Clearly mark your RFP: RFP for Support and Operate functions of Azure and Zscaler platforms for the attention of JJ Singh, Senior Technical Commercial Advisor
c. Submit your RFP before the Deadline for RFPs.
d. Your RFP must remain open for 4 calendar months from the Deadline for RFPs.
e. You can use the Response Form RFP attached

Pricing information

a. Your RFP should clearly state the total price, for full delivery, in NZ$ and exclusive of GST.
    - Please provide costing information in the attached spreadsheet: CCTV&EAC Costing Template

b. Show how you will manage risks and contingencies related to the delivery of the Requirements.
c. Document any assumptions that you have made about delivery of our requirements. State any assumption that Oranga Tamariki or a third party will incur any costs and estimate that cost if possible.
d. Your RFP must show a breakdown of all costs, fees, expenses and charges.
e. [Stipulate any additional information you require].

Terms and Conditions

The following government standard terms and conditions apply to the RFP and the RFP process:

a. you must bear all your own costs in preparing and submitting your RFP
b. you represent and warrant that all information provided to us is complete and accurate
c. we may rely upon all statements made in your RFP
d. we may amend, suspend, cancel and/or re-issue the RFP at any time
e. we may change the RFP, but will give suppliers a reasonable time to respond to the change
f. we are not bound to accept the lowest priced conforming RFP, or any RFP
g. if none of the RFPs are acceptable to us, we may enter into negotiations with one or more suppliers for a satisfactory offer
h. we both agree to take reasonable steps to protect the other's confidential information
i. our obligation to protect your confidential information is subject to the Official Information Act 1982 and other legal, parliamentary and constitutional conventions
j. there is no binding legal relationship between us, and your RFP is only accepted if we both sign a contract or if we issue a purchase order to you
k. our Request for RFPs (RFP) comprises this document, and any subsequent information we provide to suppliers
l. the laws of New Zealand shall govern the RFP and RFP process

m. in submitting your RFP, you are deemed to have read, understood and agree to be bound by these terms and conditions, and the additional terms and conditions below, if applicable.

n. In submitting your RFP, we reserve the right to go to market if we are not satisfied with the support capability, capacity or costs

View RFP Terms and Conditions here:

RFP Terms and Conditions (procurement.govt.nz)