Solomon Islands Government

Office of the Auditor-General

Special Investigation Audit Report

Into the

Passport System

National Parliament Paper No: 1 of 2021

Reported by:

Auditor-General
Office of the Auditor-General
P O Box G18
Honiara

August 2020

Table of Contents

1 Overview

1.1 Background

A recent Cyber Security review highlighted sufficient reason to suspect the Passport System may have been compromised by internal or external actors which may have resulted in unauthorised Solomon Islands passports being issued illegally.

We therefore determined a Special Investigation was required to investigate this issue. A special investigation has been accepted to Audit by the Auditor General in terms of Section 108(3) of the Constitution.

1.2 Purpose of the audit

The objective(s) of the special audit were to confirm whether there was evidence that passports were being issued illegally. To do this we sought to understand and then express an independent outcome on:

- The general control environment of the Immigration Office;
- The passport system and what controls exist, whether they are designed and operating effectively;
- The IT controls; and
- The key contracts to deliver the electronic passport (e-passport) system.

1.3 Audit approach

Due to the concerns identified during the planning of the audit, our visit was unannounced. On 5 February we arrived on site at the Passport Offices.

Our audit focused initially on the following:

- Gaining an understanding of
    - the passport processes;
    - the e-passport system; and
    - the control environment of the Immigration office (Physical and IT security).

- Capturing the data within the system to undertake analysis of passport activity.

Having undertaken this analysis we then undertook testing of the system. We undertook analysis of data collected to investigate whether passports had been issued illegally. We then tested a sample of e-passport applications to assess whether the controls within the system were operating effectively to ensure compliance with the process to issue e-passports.

Our testing was directed by weaknesses observed during our onsite observations. Specifically the testing considered whether:

- Multiple passports were issued to individuals;
- Express processing of passports was in line with fees paid;
- There was compliance with the expected processes;
- Activity of Immigration Officers out of hours related to legitimate applications; and
- Any unusual activity of Immigration Officers was occurring outside their normal user functions.

We also considered whether contracts are managed appropriately to ensure value for money is achieved for the Solomon Islands.

Procedures performed to gather evidence in answering the audit question are as follows:

- Interview and Inquiry – we have made enquiries of passport officers and management to gather information and explanation concerning specific audit matters;
- Review processes – We reviewed current processes to identify controls that should mitigate risk of misstatement;
- Inspection – We have inspected documentation including applications, evidence, and the passport system; and
- Observation – We have observed processes and controls in operation.

Our audit was conducted using a risk based approach with audit tests focusing on the risk areas leading to our findings.

1.4 Conclusion

Our testing has not found evidence of malicious actors in the system leading to the issue of unauthorised passports.

We have found systematic failure in the controls within the Immigration Office. Due to the failure of these controls this creates opportunities which could be exploited. We are therefore unable to provide assurance that passports with false information have not been issued. This severely undermines the integrity of the Solomon Islands official travel document which could restrict the future rights of Solomon Islands passport holders travelling or working offshore.

Our testing has initially identified almost 700 individuals with possible multiple biometric passports (in the e-passport system) and up to 1500 possible multiple passports from the old passport system. We undertook testing of 27 of these individuals and confirmed ten had at least two live biometric passports in issue. Of the 27, 11 were also found to have a valid passport in the old system.

These are not deemed to be isolated incidents as our analysis and testing has shown a systemic failure of key controls relating to the issue of passports. This requires immediate corrective action to be taken.

We found the contract in place for the provision of the e-passport system had not been reviewed by the Solicitor or Attorney General prior to signing. We recommend engaging with the provider to resolve some of the gaps in the contract and to ensure a firm basis from which the delivery of the service can be monitored into the future.

Due to the national significance of the passport system and the reputational damage there could be through such control failings we recommend that the Ministry develop an action plan to address these issues as a priority.

Given the significance of the issues raised we will undertake a review in 3 months to confirm immediate priority actions have been undertaken followed by a review within 1 year to ensure ongoing progress is being made.

2 Detailed findings

Our audit has revealed evidence of systematic failure in the operation of controls. Whilst we have not found evidence of fraudulent activity perpetrated by Officers or external parties within the system, we have observed that the control failures create opportunities which could be exploited by individuals to suit their purposes and are unlikely to be detected. This creates a significant issue for the Ministry which should be resolved immediately.

Our report highlights matters raised by the Ministry and matters we identified through the audit. The aim of this report is to provide as full a picture as possible so the Ministry can determine an appropriate course of action to respond and address the weaknesses.

2.1 Physical and IT security

Having undertaken this audit unannounced, we were able to assess the control environment of the Ministry. Our visit revealed a poor level of physical security over core passport processing functions and the system:

- The entrance door to the unit was unlocked despite security features being installed.
- The door from the public space was open so the public can come in for their photos but this meant they could then access the rest of the Office and have easy access to passports available for collection.
- There is no security in operation to the rooms where the blank passports and printing machine are held.
- The server room for the passport system is unlocked.
- Neither the blank passports nor the printed ones for collection were stored securely.
- Old application files are stored in boxes across the Office in areas which although shouldn't be, could be accessed by the public.

From an IT security perspective, passwords are a key control to ensure access to a system is controlled to only those authorised. They also provide a control to ensure segregation of duties. This is a key control in preventing unauthorised activity in a system.

We found that individual's shared their passwords with other staff to facilitate their access to a system. An example of this is if someone's account was locked and the administrator was not available to reset it, then other staff would provide their password so the individual could continue with their work.

As passwords are not regularly changed, this means that these passwords are known within the team and could allow individuals to access the whole system providing the opportunity to undertake unauthorised processing.

We also found that one of the Officers had the Administrator password which did not align with their user rights. Whilst this individual demonstrated good security of the password, they none the less had it and used it to access the system.

#	Rating	Recommendation
1	**High**	**Review the physical and IT security measures and develop a plan to address any deficiencies.**
2	**High**	**Enforce existing physical and IT security measures which are in place are operating.**
3	**High**	**Re-set IT security passwords. Ensure all staff understand that under no circumstances should they share their passwords.**
4	**High**	**Implement appropriate measures around password security to ensure if anyone is locked out, this can be rectified in a timely manner.**
5	**High**	**Review the access rights associated with each member of staff to ensure that it appropriately reflects their role within the process.**

2.2 Contract

We undertook a review of the contract in place for the e-Passport system. This included using expertise of the Solicitor General and the Ministry of Finance's procurement team. Our review has concluded that there is an uneven balance to the contract in favour of the provider and the contract does not address some key elements we would normally expect. Overall, we are seriously concerned that the contract was entered into in this form.

To illustrate this we have detailed two examples below:

Contractual clause	**Audit Observation.**
The price of the contract is set out in Schedule C. This states: *Minimum orders and price:* *Electronic passport: 10,000 units per year (agreed unit price of the electronic passport: USD 110.00)*	Data from the e-passport system shows that approximately 5500 passports were issued in 2018 and 2019. Pricing the contract on the basis of passports is leading to a position that blank passports are being stockpiled as the Ministry tries to keep up with the minimum order requirements, despite not needing this level of passports. This creates a security issue. We recommend the number of passports required should be right sized and if necessary, the payment mechanism should be reviewed.
Allocation of risk *5.1.1(b) – the Government shall pay IRIS liquidated damages of such amount equivalent to the total sum receivable in the next 5 year period by IRIS under this BOT Agreement as if all the Products were delivered to the Government minus actual sum paid by the Government and received by IRIS for all Products up to the date of termination.* *10.1.1 - IRIS Corporation is to control any pending litigation by a third party and SIG will pay any subsequent award but only with the consent of IRIS Corporation.*	The liquidated damages are significantly balanced in the favour of IRIS. $10,000 USD liability on the part of IRIS does not provide sufficient penalties to warrant good performance from the supplier in contrast to the 20-year contract term. This is particularly so when considered in conjunction with section 10.1 where IRIS controls the process for any litigation with the Government.

14.1 - IRIS's entire liability… shall not exceed USD $10,000	This is compared to the costs for the Government to terminate the contract no matter the reason (and this includes force majeure which would normally be nil penalty) at $5.5m USD.

We have discovered that the contract was not reviewed by the Solicitor General or Attorney General prior to signing. This is not good practice. By not complying with seeking the right advice, the outcome for the Solomon Islands is a contract which is unfairly balanced to the provider and poses a number of risks.

We recommend that the Ministry engages with the provider to seek a review of the clauses within the contract to see if some of the gaps and risks can be addressed.

#	Rating	Recommendation
6	**Moderate**	**Undertake a review of the contract and the provider's performance and consider the options available to address the serious weaknesses in the contract. Ensure appropriate legal advice is sought.**

2.3 Contract management

Through undertaking the investigation we discovered that key activities we would expect to have been undertaken as part of maintenance of the system have not occurred:

- Database maintenance – the database logs on the SLBCENTRAL database which is one of the two primary passport application processing systems is currently at 400Gb.This indicates that no database maintenance or monitoring has been performed for some time. The immigration database logs are 400x higher than industry best practice for production systems, which is under 100Mb for optimal performance.
- Database backups have not worked since April 2019 – the immigration databases have not been backed up for almost a year as the backup drive is at capacity. A critical systems failure now would mean a catastrophic loss of all transactions processed since the last backup or in worst case, the entire

dataset which could have a critical impact on the functioning of border control. [1]

- The Windows Server license had lapsed – the database servers for IRIS is running on an unlicensed Windows Server operating system. This means that there is no support for critical patches to address software bugs or security vulnerabilities.
- Database software is out of support – the database the passport system is running on is Microsoft SQL Server 2014 which is out of support since 2016. This also means that there is no support for critical patches to address known software bugs or security vulnerabilities.
- Signs of imminent hardware failure – when attempting to perform backups, we experienced unusual errors which indicate that either the hardware controller or hard drive array [2] may be failing. Should it fail, it would lead to catastrophic failure of the system and data and the lack of backup would make it extremely difficult to recover any data, or result in an extended outage of the IRIS system.

It is our view that these issues demonstrate that the supplier has breached its stated obligations under the contract in relation to the basic systems maintenance or preventive maintenance.

In addition whilst we were on site the printer was not working causing temporary paper passports to be printed. Through testing we discovered that the scanner was not producing scans that were legible. These types of issues should have been immediately reported to the provider so they can take action to ensure the ongoing functioning of the system to avoid the kind of workarounds which are in place and are inadequate.

Given the absence of any service level agreements in the contract, there is no regular monitoring of the provider performance other than through the delivery of passports. Good contract management involves "tracking and monitoring delivery and costs, managing risks and relationships, conducting reviews and resolving problems managing performance during delivery[3]". In the absence of a specified framework to monitor performance, the Ministry should review the contract to understand the service and establish its own mechanisms to monitor performance.

[1] Note that our specialist IT auditors had to intervene by initiating a full back up on 5 February 2020 to help to mitigate the risk of catastrophic systems failure and data loss, but not all databases were successfully backed up.

[2] Hard drive array is a data storage system used for block-based storage, file-based storage or object storage.

[3] New Zealand Government Procurement: A guide to procurement.

#	Rating	Recommendation
6	**Moderate**	**Undertake a review of the contract and the provider's performance and consider the options available to address the serious weaknesses in the contract. Ensure appropriate legal advice is sought.**
7	**Moderate**	**Ensure that deficiencies in the provision of the e-passport system are raised with the provider in a timely manner.**
8	**Moderate**	**Determine appropriate measures of performance and implement contract monitoring and management arrangements.**

2.4 Opportunities to strengthen the passport process

We discussed the system with the Chief Immigration Officer and some of the Immigration Officers and observed how they processed passport applications. Through these observations, our walkthroughs of the system and testing undertaken we identified a number of issues with the process.

2.4.1 Evidence required to support an application

The application form allows either a Birth Certificate, 2 signed statements or a Birth Notice to be submitted with the application form as evidence of the applicant's date of birth.

During the review, the Ministry raised their concern with us that the Birth Certificates were not a reliable document to evidence an applicant's date of birth. As a result they have ceased to accept these. During our review, we observed that the 2 signed statements are also not a reliable source of evidence with a number of fraudulent applications being pointed out to us. The Ministry have observed that they have little other reliable evidence to rely on to verify the date of birth.

In a similar way, concerns were raised around the evidence of citizenship for some applicants. In one instance provided to us during the audit, a certificate had been provided by the applicant and identified by Officers as fraudulent. This was confirmed when they consulted the Ministry of Home Affairs. Whilst this instance was successfully identified and a passport was not issued, the absence of a control which requires consultation with the Ministry of Home Affairs means that other such instances may not all be identified. Implementing a requirement to check all citizenship status with the Ministry of Home Affairs would strengthen the process.

#	Rating	Recommendation
9	Moderate	**Undertake a review of the evidence required to demonstrate Date of Birth. Update legislation, regulations and the application forms for the process accordingly.**
10	High	**Consider implementing a control which verifies the accuracy of statements provided in the process to confirm date of birth and citizenship.**

2.4.2 Multiple passports in circulation

The system will flag to an Officer when duplicate applications are being processed. One such example is if a finger print is already allocated to a passport in the system. However our audit found that some of these controls can and are being overridden.

We therefore undertook testing and have confirmed that there are a large number of citizens with multiple passports in issue.

The most common scenario which can cause this is when an applicant requests a new passport. If the system identifies that they already have a valid passport in issue, the Officers will cancel that application and re-process it as a new application following a lost passport and override the system warning. For the new application following a lost passport, the applicant has to provide evidence their original passport is lost (by providing a police report) and pay an additional fee.

Our testing of 27 applicants found that 10 of them had more than one valid passport in issue. The part of the process which seems to be missing is that when the new passport is created, the old one which is lost should be cancelled. The risk therefore is that malicious actors could gain access to a lost passport which is still valid.

This is further complicated by the fact that our observations of the process noted that the process to damage the old or erroneous passports, to show they are cancelled, was not effective.

During the review we asked to see examples of how erroneous passports printed were cancelled. We found that they had not been physically marked to show cancellation. Furthermore, there seemed to be some confusion as to how the biometric passports should be marked to note their cancellation.

Our testing identified a couple of applicants that made multiple applications in a short period of time. In one instance, this was not in relation to a lost passport and appeared that the individual simply wanted a new passport. It is unclear why this would be necessary and poses the question whether there is any malicious intent behind this.

#	Rating	Recommendation
11	**High**	**Review the cases provided by audit to determine if multiple passports for individuals are in issue and ensure the system is updated to cancel the version which is old, replaced and no longer valid.**
12	**High**	**Liaise with the Supplier to confirm how:** • **Lost or replaced passports should be treated in the system and undertake training for staff to ensure this doesn’t occur in future.** • **Erroneous or invalid passports should be marked to ensure their cancelled status is clear.**

2.4.3 System overrides

The ability to override an alert built into the system was also noted in other areas:

- A finger print is required as part of the biometrics. If the scanner won’t read the fingerprint it can be processed without the fingerprint.
- A finger print is required to collect a passport. If the individual isn’t there or the fingerprint reader not working, the passport can be issued anyway.

Finger print controls are built into the system as a means of having a unique identifier. By overriding the controls, Officers remove the ability to have this unique identifier and reduce the effectiveness of the control.

We found that although there is space in the system to record decisions, whether it is due to an override or another reason, the comments on the system are brief and often do not provide sufficient information to understand the decision making. As a result Officers usually record these on the manual application forms. Our audit found that these forms, once processed are not stored securely or in order and are therefore hard to locate to evidence and audit the decision making.

#	Rating	Recommendation
13	High	**Consider building in controls which reviews where warnings have been overridden so that any errors can be detected early and corrective action taken if necessary.**

2.4.4 Unusual processing

One of the possible indicators of fraudulent processing would be that one individual undertakes more of the process than normal or that they process the application out of normal hours.

We undertook testing to see if there was any evidence of such activity. Whilst we found no evidence of processing fraudulent passports we did find evidence of both these practices. Although we are unable to prove these activities were done with criminal intent, we are concerned that staff may have been put under pressure by members of the public service or wider community to process applications quickly and that this may be masking malicious or criminal intent. By acceding to such requests staff are left vulnerable to accusation when their activity may have been innocent.

Similarly, applicants can apply for express processing which will generally mean the passport will be ready within 5 days. We undertook analysis of processing to see if there was any indication that Officers were inappropriately fast-tracking applications. We found that for each application tested processed under 5 days, an express fee had been paid.

Officers explained to us that they generally attempt to respond to the urgency of the applicant and would therefore process within 24 hours if a departure was imminent. Whilst this shows a flexibility to customer service we noted that the Officers do not necessarily sight or retain evidence of the imminent departure and therefore the speed may be more self-interested or by the individual’s poor planning. By prioritising such instances there is a risk that others are unnecessarily delayed, or that thorough investigation does not occur.

#	Rating	Recommendation
14	Moderate	**Out of hours activity should be reduced to a minimum.**

		Develop an exception report which identifies any activity undertaken out of hours which should be reviewed independently. Unusual activity should be investigated and explained.

2.5 The old passport system

Whilst our focus has been on the operation of the new e-passport system, we have considered how the old system is being used.

The e- passports have been in issue since 2017, gradually replacing the old manual versions. The policy is that as an old passport expires, applicants can apply for a new biometric one. This means that over the period to 2026, the old passports will be phased out.

The Ministry informed us however that there have been occasions during the operation of the new biometric passports when the system wasn’t operating (in one instance due to a shortage of biometric passports) which resulted in the old manual passports being issued instead. This means that the system may need to be maintained longer than 2026.

Through the audit we have observed a number of concerns with the ongoing operation of the old system:

- The old system is operated on Windows XP. This is unsupported and therefore at risk of being compromised due to known security vulnerabilities.
- The old system has not been backed up and given its age, there is a high likelihood that the system could fail (e.g. a hard drive crash) prior to 2026, resulting in loss of the passport database.
- We understand that Officers check the old system to confirm any information in an application and ensure the old passport has expired. During our visit we found that this may not occur consistently and as there is no evidence of this, it is not designed effectively as a control.
- Our testing has initially identified almost 1,500 individuals with possible multiple passports in the old passport system.
- Furthermore, our testing of the 27 applications for biometric passports found 11 individuals who had valid passports in both systems. Given our concern that old passports may not be effectively cancelled when issuing a

new one, there is a risk that these old passports may still be in useable circulation.

We are aware of passports in worldwide use which are attempting to copy the old passport system. These are notified to Immigration as required. Given the increasing number of such instances, we recommend that the Ministry reviews whether it is appropriate to maintain this old system.

#	Rating	Recommendation
15	**High**	**Review all passports issued in both systems to cancel with immediate effect any instances where citizens are recorded as having multiple passports within or between systems.**
16	**Moderate**	**Given the instances of fraud which are being reported to the Ministry through worldwide activities, undertake a review whether the old passport system should be phased out sooner than currently planned.**
17	**Moderate**	**Build in an effectively designed control which ensures the verification of the old passport system for any valid passports prior to issuing one within the new passport system. This could be evidenced by a print out from the system which is then attached to the application form and scanned as part of the evidence to the e-passport system. This should also include the cancellation of any replaced passports in the old system when one is issued in the new.**

Appendix 1: Recommendation rating definition

A description of the ratings as applied to our recommendations is set out below:

Priority Rating	Description of impact
High	• Matters which may pose a significant business or financial risk to the entity; and / or • Matters that have resulted or could potentially result in a modified or qualified audit opinion if not addressed as a matter of urgency by the entity; and / or • Moderate risk matters which have been reported to management in the past but have not been satisfactorily resolved or addressed.
Moderate	• Matters of a systemic nature that pose a moderate business or financial risk to the entity if not addressed as high priority within the current financial year; and / or • Matters that may escalate to high risk if not addressed promptly; and / or • Low risk matters which have been reported to management in the past but have not been satisfactorily resolved or addressed.
Low	• Matters that are isolated, non-systemic or procedural in nature; and / or • Matters that reflect relatively minor administrative shortcomings and require action in order to improve the entity's overall control environment.
Improvement Opportunity	• Matters of a procedural or administrative nature which could improve the efficiency or effectiveness of entity level, systemic or transactional processes.

Appendix 2: Recommendations action plan

Audit Issue	OAG Recommendations	Detail Action that is to be / has been Taken	Responsible Officer	Target Date	OAG Response
Physical & IT security	1. Review the physical and IT security measures and develop a plan to address any deficiencies. 2. Enforce existing physical and IT security measures which are in place are operating. 3. Re-set IT security passwords. Ensure all staff understand that under no circumstances should they share their passwords. 4. Implement appropriate measures around password security to ensure if anyone is locked out, this can be rectified in a timely manner. 5. Review the access rights associated with each member of staff to ensure that it appropriately reflects their role within the process.	Immigration had liaised with Iris Corporation Berhad in Malaysia to review the IT security Request to have Electronic door for passport office approved by DOI/PS Action has been taken to re-set IT security Passport Relocated of password to passport officers already done Re-allocated of each officer to each workflow station and	Iris Company engineer Patrick Fataga, MCILI, PIO Director of Immigration (DOI) Director of Immigration Chief Immigration Officer Passport	5-9 Oct. 20 3-14 Aug. 20 20 July 20 Ongoing process 18 May 20	OAG acknowledges the proposed actions and will follow-up progress to monitor implementation.

		processes of e-passport has been done			
Contract Management	1. Ensure that deficiencies in the provision of the e-passport system are raised with the provider in a timely manner. 2. Determine appropriate measures of performance and implement contract monitoring and management arrangements.	Imm to liaise with PMO & AG to review the contract with Iris Company Imm to liaises with PMO and Attorney General to review the Contract with Iris Corporation Berhad	PMO/AG/Iris Comp Berhad PMO, AG & Iris Corporation Berhad	16 Nov. 20 16 Nov. 20	OAG acknowledges the proposed actions and will follow-up progress to monitor implementation.
Evidence required to support an application	1. Undertake a review of the evidence required to demonstrate Date of Birth. Update legislation, regulations and the application forms for the process accordingly. 2. Consider implementing a control which verifies the accuracy of statements provided in the process to confirm date of birth and citizenship.	Application forms and Date of birth document revised Legislation & regulation approved for review Renewed approaches and revised requirement already established	CIO/PPT Immigration, AG & PIDC Imm, Citizenship & Birth Registry	2-31 Mar. 20 Jan- March 21 3 Feb. 20	OAG acknowledges the proposed actions and will follow-up progress to monitor implementation.

Multiple passports in circulation	1. Review the cases provided by audit to determine if multiple passports for individuals are in issue and ensure the system is updated to cancel the version which is old, replaced and no longer valid. 2. Liaise with the Supplier to confirm how: • Lost or replaced passports should be treated in the system and undertake training for staff to ensure this doesn't occur in future. • Erroneous or invalid passports should be marked to ensure their cancelled status is clear.	Proposal to review the issue of multiple passports in circulation has been submitted to Iris Corporation Berhad Company already and response was positive Immigration strategically address the technical issue with the Vendor and agreed to troubleshoot the issue. Capacity training bid approved to undertake training in Malaysia Measure to cancelled invalid Passports enforced.	Iris Corporation Berhad engineer/Imm Iris Corporation Berhad 2 Imm officers CIO/Ppt	Jan. 21 (on progress) Jan- Dec 21 Ongoing process Sept. 20 31 Mar. 20	OAG acknowledges the proposed actions, however, we are concise that the date to start resolve the issue is 2021 and the potential training in 2020 will be likely hindered as a result of COVID19. Risks associated with this issue are high therefore we continue to recommend this issue is addressed urgently.
System overrides	1. Consider building in controls which reviews where warnings have been overridden so that any errors can be detected early and corrective action taken if necessary.	Only DOI to approved application for override before an immigration officer passport perform issuance	DOI/ immigration officer	1 June 20 ongoing process	OAG acknowledges the proposed actions and will follow-up progress to

					monitor implementation.
Unusual Processing	1. Out of hours activity should be reduced to a minimum. Develop an exception report which identifies any activity undertaken out of hours which should be reviewed independently. Unusual activity should be investigated and explained.	Processing of passports start from 9:30am – 4:30 pm. Only genuine applications with legitimate documents would have process out of hours	CIO-Passport and Imm Officer ppt	1 June 20	OAG acknowledges the response, however, we note that the response does not effectively mitigate risks of processing after working hours.
The old passport system	1. Review all passports issued in both systems to cancel with immediate effect any instances where citizens are recorded as having multiple passports within or between systems. 2. Given the instances of fraud which are being reported to the Ministry through worldwide activities, undertake a review whether the old passport system should be phased out sooner than currently planned. 3. Build in an effectively designed control which ensures the verification of the old passport system for any valid passports prior to issuing one within the new passport system. This could be evidenced by a print out from the	Renewed approached has been implemented. Regular check on old system conducted. Person found having multiple passports both new and old must cancelled either, and in possession of one legal passport Immigration authority will liaises with AG for advice to conduct mass cancellation of those citizens who are still in possession of old passports Prescribed administrative practice in production of renewal	CIO-PPT/Imm Officers CIO/DOI & AG	6 June 20 3 Jan 21	OAG acknowledges the proposed actions and will follow-up progress to monitor implementation.

	system which is then attached to the application form and scanned as part of the evidence to the e-passport system. This should also include the cancellation of any replaced passports in the old system when one is issued in the new.	of old passports has been executed with constricted observation by the Chief Immigration Officer-passport. Should passport holder of old passport wishes to apply for a new e-passport, he/she must submit the current passport for cancellation and evidence before passport application could process. In the event where the passport holder lost his/her passport police report must provide for facilitation	CIO and Immigration Officers- Passport	Ongoing process	

Appendix 2a: Recommendations action plan update as at 18/11/2020[4]

Audit Issue	OAG Recommendation	Immigration Response
Physical & IT security	1. Review the physical and IT security measures and develop a plan to address deficiencies 2. Enforce existing physical and IT security measures which are in place are operating 3. Re-set IT security passwords. Ensure all staff understand that under no circumstance should they share their passwords 4. Implement appropriate measures around password security to ensure if anyone is locked out, this can be rectified in a timely manner 5. Review the access rights associated with each member of staff to ensure that it appropriately reflects their role within the process	On process with Vendor Done Done Done Done
Contract Management	1. Ensure that deficiencies in the provision of the e-passport system are raised with the provider in a timely manner 2. Determine appropriate measures of performance and implement contract monitoring and management arrangements	On process On process
Evidence required to Support an application	1. Undertake a review of the evidence required to demonstrate Date of Birth. Update legislations, Regulations and the application forms for the process accordingly 2. Consider implementing a control which verifies the accuracy of statements provided in the process to confirm date of birth and citizenships	Done Done

[4] OAG is yet to do a follow up audit to verify this.

Multiple passports in circulation	1. Review the cases provided by audit to determine if multiple passports for individuals are in issue and ensure the system is updated to cancel the version, which is old, replaced and no longer valid 2. Liaise with the Supplier to confirm how: • Lost or replaced passports should be treated in the system and undertake training for staff to ensure this does not occur in future • Erroneous or invalid passports should be marked to ensure their cancelled status is clear	On process with technical expertise (Vendor) Done (immigration officers undertake trainings) Done (systematic administrative measure in place)
System overrides	1. Consider building in controls which reviews where warnings have been overridden so that any errors can be detected early, and corrective action taken if necessary	Done (Director grant approval before immigration officer perform override)
Unusual Processing	1. Out of hours activity should be reduced to a minimum. Develop an exception report which identifies any activity undertaken out of hours which should be reviewed independently. Unusual activity should be investigated and explained.	Done (immigration officer - passport does not allow to perform processing of passports after working hours except on special cases)
The old Passport System	1. Review all passports issued in both systems to cancel with immediate effect instances where citizens are recorded as having multiple passports within or between systems 2. Given the instances of fraud which are being reported worldwide activities, undertaken a review whether the old passport system should be phased out sooner than currently planned 3. Build in an effectively designed control which ensures the verification of the old passport system for any valid passports prior to issuing one within the new passport system. This could be evidenced by a printout from the system which is then attached to the application form and scanned as part of the evidence to the e-passport system. This should also include the cancellation of any replace passport in the old system when one is issued in the new. Submit the current passport for cancellation and evidence before passport application could process. In the event where the passport holder lost his/her passport police report must provide for facilitation	Done (renewed approach established) Proposal to phase out the old system still on process Done (prescribed administrative mechanism in force to control production of renewal of old passports)

Appendix 3: Detail of exceptions

This information will be provided separately due to the confidential nature of the data.