INFORMATION SECURITY AUDIT

OF

ROYAL MONTSERRAT POLICE SERVICE

OVERSEAS TERRITORIES REGIONAL CRIME INTELLIGENCE SYSTEM (OTRCIS)

2008 - 2019

Office of the Auditor General
Brades, Montserrat

February 2020

INFORMATION SECURITY AUDIT OF THE ROYAL MONTSERRAT POLICE SERVICE:

OVERSEAS TERRITORIES REGIONAL CRIMINAL INTELLIGENCE SYSTEM (OTRCIS)

This is a Report of an Information Security (IS) Audit conducted by the Office of the Auditor General

Florence A. Lee
Auditor General
Office of the Auditor General
February 2020

PREAMBLE

Vision Statement

"To be a proactive Supreme Audit Institution that helps the nation make good use of its resources."

Mission Statement

"The O.A.G is the national authority on public sector auditing issues and is focused on assessing performance and promoting accountability, transparency and improved stewardship in managing public resources by conducting independent and objective reviews of the accounts and operations of central government and statutory agencies; providing advice; and submitting timely Reports to Accounting Officers and the Legislative Assembly."

The Goal

"To promote staff development, enhance productivity, and maintain a high standard of auditing and accounting in the public sector, thereby contributing to the general efficiency and effectiveness of public finance management."

AUDITOR GENERAL'S OVERVIEW

We conducted an Information Security Audit of the Overseas Territories Regional Criminal Intelligence Systems (OCTRIS) software. The objective of this review was to establish if the OCTRIS software and the related computer and communication systems are properly secured against unauthorized access and modification of information whether in storage, processing or transit, and against denial of service to authorised users.

In relation to the software itself, we found that it was robust and secure with stringent policies, procedures and controls that prevents unauthorized access and modification of data. However, we found a number of issues that need to be addressed to make the system more effective. These included (a) Non-operational Door Access Control and external surveillance Camera Systems; (b) Insufficient Fire Suppression Apparatus; (c) Redundant Emergency Systems; and (d) Lack of Backup Power Supply.

Several recommendations were tendered to address these Environmental and Physical Access related weaknesses/shortcomings. Once implemented, they would strengthen those security controls.

Florence A Lee
Auditor General
Office of the Auditor General
Angelo's Complex,
Brades, Montserrat
February 2020

TABLE OF CONTENTS

PREAMBLE ..... **II**

Vision Statement II
Mission Statement II
The Goal II

AUDITOR GENERAL'S OVERVIEW ..... **III**

ABBREVIATIONS ..... **V**

EXECUTIVE SUMMARY ..... **VI**

CHAPTER 1 INTRODUCTION **1**

Audit Objective 1
Management Responsibility 1
Auditor's Responsibility 1
Audit Mandate 1
Audit Standards & Guidelines 1
Audit Scope and Methodology 2

CHAPTER 2 BACKGROUND **3**

Overseas Territories Regional Crime Intelligence System 3
Royal Montserrat Police Service 3
Legal Framework 3
Montserrat Integrated Border Security Unit 3

CHAPTER 3 OUTSOURCING **5**

Service Level Agreements and Contracts 5
Ownership and Data Rights 6
Intellectual Property 6

CHAPTER 4 INFORMATION TECHNOLOGY OPERATIONS **7**

Problem and Incident Management 7
Change Management 7

CHAPTER 5 INFORMATION SECURITY **8**

Human Resources Security 8
Physical Access Controls 10
Environmental Security 11
Logical Access Controls. 12
Communications and Operations Management 15

CHAPTER 6 APPLICATION CONTROLS **17**

Input and Processing Controls 17
Output Controls 20

CHAPTER 7 DISASTER RECOVERY AND BUSINESS CONTINUITY **21**

Disaster Preparedness Plan 21
Backup and Recovery 21

CHAPTER 8 FINDINGS AND RECOMMENDATIONS **22**

Findings 22
Recommendations 23

CHAPTER 9 CONCLUSION **24**

REFERENCES **26**

APPENDICES **27**

APPENDIX I - OTRCIS Network Diagram *28*
APPENDIX II - OTRCIS Client, Installation, and Login Windows *29*
APPENDIX III - Non-Operational Fire Alarm System & Mounting Hook for Missing Fire Extinguisher *30*
APPENDIX IV - Outer Cover of Defunct Emergency System Control Panel *31*
APPENDIX V - Interior of Defunct Emergency System Control Panel *32*
APPENDIX VI - Other RMPS Server Room Equipment *33*
Appendix VII - Various Physical & Environmental Controls at Brades Police HQ *34*

ABBREVIATIONS

BOT	British Overseas Territories
COT	Caribbean Overseas Territories
DITES	Department of Information Technology and e-Services
ES	Emergency System
FCO-OTD	Foreign Commonwealth Office - Overseas Territories Dependencies
GoM	Government of Montserrat
GUI	Graphical User Interface
HR	Human Resource
HRMU	Human Resources Management Unit
IBSU	Integrated Border Security Unit
ISAE	International Standard on Assurance Engagements
ISSAI	International Standard of Supreme Audit Institutions
IS	Information Security
IT	Information Technology
MCD	Montserrat Customs Division
MFRS	Montserrat Fire and Rescue Service
MUL	Montserrat Utilities Limited
OAG	Office of the Auditor General
ODG	Office of the Deputy Governor
OTRCIS-CIM	Overseas Territories Regional Criminal Intelligence System - Crime Intelligence and Management
RMPS	Royal Montserrat Police Service
SA	System Administrator
SLA	Service Level Agreement
SOP	Security Operating Procedures
Supt.	Superintendent
UK	United Kingdom
URN	Unique Reference Number

EXECUTIVE SUMMARY

Overview

1. The Overseas Territories Regional Crime Intelligence System (OTRCIS) is a networked computerised system that was developed in 1996 by MEMEX Technology Limited and designed to assist the British Caribbean Overseas Territories (Anguilla, British Virgin Islands, Cayman, Montserrat, and Turk & Caicos) Police, Customs, and Immigration Departments in the prevention, detection, and investigation of major crime. The Royal Montserrat Police Service (RMPS) commenced utilising the OTRCIS software, circa 1998/1999, to gather and share information with the other Caribbean Overseas Territories (COTs).

Key Findings

2. Very secure software. OTRCIS software is very robust and secure with very stringent policies, procedures, and controls in place that ensure the safeguarding of OTRCIS-related computer equipment; and the data that is inserted in the forms, stored on the server, and transmitted across the network; against unauthorised access and modification.

3. Non-operational Door Access Control and External Surveillance Camera Systems. The buzzer door system for controlling the traffic in and out of office areas at Brades Police Headquarters, and the external security camera system have been non-operational for several years.

4. Insufficient Fire Suppression Apparatus. Inspections of the main foyer area and IT and Server Rooms at the Brades Police Station, revealed that there are either missing, or no electrical fire extinguishers, installed in either of these spaces.

5. Redundant Emergency System. There is an Emergency System (ES) comprised of fire alarms, smoke detectors, and temporary lock-up (or jail) cell buzzers, installed at the Brades Police Station that was disconnected approximately three to four years ago by the vendors, after it malfunctioned.

6. Lack of Backup Power Supply. It was noted that the computer equipment at the Salem Police Station are not protected against power outages, surges, spikes, burnouts, or temporary loss of information, by backup sources of power such as a backup generator and interactive-line UPSs. However, it was indicated that the RMPS has future plans to resolve the current situation.

Recommendations

7. **Replacement of Door Access Control and Surveillance Cameras Systems**. We are recommending that the RMPS renew their effort of procuring replacements for the non-operational front buzzer door and external security camera systems with either a keycard based door access control system that generates audit trails; and/or one that is combined

with both internal and external camera surveillance. Another option is a biometric security system with fingerprint or hand geometry readers, or facial recognition scanners.

8. **Replacement Equipment**. We are recommending that fire extinguishers be installed in the Server and IT Rooms, and foyer; and for the Emergency System to be reinstated for the early detection and warning of smoke and fire; and facilitation of distress calls from the jail cells.

   At the Salem Police Station there is a need for Line-interactive UPSs to safeguard against data loss and to protect the computer equipment from power surges, spikes, and burnouts; and a backup generator to supply a steady, reliable, source of electricity during power outages or other emergency situations.

Audit Conclusion

9. The Office of the Auditor General (OAG) has concluded that the OTRCIS software is a very robust and properly secured against unauthorised access and modification of information. This was achieved by the establishment of very stringent Outsourcing, IT Operations, Application, Information Security, Disaster Recovery and Business Continuity policies, procedures, and controls by both the contractor and RMPS.

   The only weaknesses that were found were Environmental and Physical Access related factors; it is advisable that the RMPS consider and address the highlighted shortcomings and recommendations in a timely manner.

THIS PAGE WAS LEFT BLANK INTENTIONALLY

CHAPTER 1 INTRODUCTION

1. The Overseas Territories Regional Criminal Intelligence System (OTRCIS) has been in existence since 1998 and is utilised for the gathering and disseminating of information amongst the Caribbean Overseas Territories.[1] The Royal Montserrat Police Service (RMPS) commenced utilising the OTRCIS software, circa 1998/1999.

Audit Objective

2. The objective of this Information Security (IS) review was to establish if the OTRCIS software and the related computer and communication (internal & external) systems are properly secured against unauthorised access and modification of information whether in storage, processing, or transit, and against denial of service to authorised users.

Management Responsibility

3. Management is responsible for ensuring that appropriate policies and effective controls exist. More specifically, management must ensure that policies and controls exist to facilitate IT Operations, Outsourcing, Information Security, and to guide the development of Business Continuity planning. Management is also responsible for establishing appropriate Application Controls and for ensuring that they function effectively.

Auditor's Responsibility

4. Our responsibility is to independently express a conclusion on Information Technology Operations, Information Security, Business Continuity, and Application Controls for the Royal Montserrat Police Service, based on our audit. Our work was conducted in accordance with International Standard of Supreme Audit Institutions (ISSAI) 100, 5300, and International Standard on Assurance Engagements (ISAE) 3000. These principles require that we comply with ethical requirements and plan and perform the audit in order to obtain reasonable assurance whether tried and true policies, plans, procedures, and internal controls exist and are functioning effectively, proper records have been and are being kept, and all the necessary information and explanations for the purpose of our audit, has been obtained.

Audit Mandate

5. The Office of the Auditor General (OAG) is mandated through the Montserrat Constitution Order 2010 to perform the audit. This mandate is supported by ISSAI 1, 200, 300, 400, and strengthened by the Revised Laws of Montserrat CAP 17.07 Public Finance Management and Accountability Act (PFMAA).

Audit Standards & Guidelines

6. The standards and guidelines used to assess the IT Operations, Outsourcing, Information Security, Business Continuity, and Application Controls assessments included the use of ISSAI 1, 100, 3100, 4100, 5300, and 5310, together with the IDI Handbook for IT Audits.

[1] *http://www.uniset.ca/microstates/pfpp.pdf*

Audit Scope and Methodology

7. The study covered the period January 2008 to July 2019 and focused on the examination of the policies, procedures, and controls that guide the operations, application, outsourcing, physical & environmental, logical access, security and business continuance for the OTRCIS.

8. A combination of techniques were utilised to gather information and assess whether relevant controls existed, were implemented, and if they were effective in ensuring that the RMPS's data and assets are protected and that there is continuance of service. These included, but were not limited to, interviewing of the key stakeholders from Royal Montserrat Police Service, and other relevant personnel. Other measures included inspection of documents and assets, in order to gather in-depth information about OTRCIS.

9. The findings of this report were discussed with the Commissioner of Police and the RMPS OTRCIS System Administrator; their views were taken into consideration when finalising the report.

CHAPTER 2 BACKGROUND

Overseas Territories Regional Crime Intelligence System

10. The Overseas Territories Regional Crime Intelligence System (OTRCIS) is a networked computerised system that was developed in 1998 by MEMEX Technology Limited. It was designed to assist the United Kingdom's (UK) Caribbean Overseas Territories (COTs) Police, Customs, and Immigration Departments in the prevention, detection, and investigation of major crime, such as drugs-related, fraud, and money-laundering. In 2010, the Miami-based MEMEX merged with SAS Institute Inc.; and the organisation works closely with other regional jurisdictions and United States agencies.

11. The OTRCIS database is shared by the COTs Anguilla, British Virgin Islands, Cayman, Montserrat, and Turk & Caicos, along with other British Overseas Territories (BOTs) such as St Helena and Ascension. [2,3,4] Originally, OTRCIS was based in Barbados; however, in 1997 it was gifted to the BOTs with the agreement that the Territories would fund the system by themselves.

Royal Montserrat Police Service

12. Before the introduction of OTRCIS in Montserrat, the RMPS employed a manual paper-based system for the recording and reporting of local crimes, such as deaths, murders, traffic accidents, robberies, etc., and other incidents to include extraditions, monitoring the movement of persons in the region, and of air and sea vessels, in and out of Montserrat.

13. Approximately forty (40) Police men and women, to include the Immigration Officers who were sworn-in as Police Officers, are authorised to have access to and use OTRCIS to perform the above mentioned tasks.

Mission and Vision Statements

14. The RMPS's mission is, "*To respond effectively to an ever-changing environment by the delivery of enhanced policing service for the safety and protection of the Montserrat Community*", and their vision is, "*To be recognised as a professional, effective, and efficient police service*."

Legal Framework

15. The RMPS and Immigration Department are mandated by the *CAP 10.01, Police Act.* The use of OTRCIS is regulated by the *UK Data Protection 1998, the UK Human Rights Acts,* and other relevant Territorial and International laws.

Montserrat Integrated Border Security Unit

16. The Montserrat Integrated Border Security Unit (IBSU) was a pilot project initiated by the previous Government comprised of the RPMS, Immigration Department, and Montserrat

[2] *Partnership for Progress and Prosperity, Britain and the Overseas Territories, Presented to Parliament by the Secretary of State for Foreign and Commonwealth Affairs by Command of Her Majesty, March 1999*

[3] *http://www.bbc.com/10405397*

[4] *https://web.archive.org/web/20110426124243/http://www.sas.com/news/preleases/Memex.html*

Customs Division (MCD). It was initiated by a Cabinet Decision in 2013, *"…to maximise the use of coordinated resources for control, security, and reducing border vulnerabilities and improve efficiency by streamlining the entry and exit procedures if visitors and residents of Montserrat…"*[5] However, given that the Unit was never officially established, the duties and authorities of the Customs Officers still fall under the remit of *CAP 17.04 Customs (Controls Management) Act* and the Immigration Officers, the *Police Act*.

17. There are approximately twelve authorised users in the Immigration Department, of which there are five main Officers who perform the following day-to-day tasks in OTRCIS:

- Record and monitor the movement of persons via air and/or sea vessels, in and out of Montserrat.
- Record the extensions of stay that have been granted to non-residents that live on Monserrat; or persons that have work permits and require more time to stay.
- Register the number of expats who own homes on Montserrat, to ensure that courtesies are extended to them each time they return to the island. They are usually granted the maximum stay of one (1) year.
- Provide the Office of the Deputy Governor (ODG) with information about non-Nationals that apply for Permanent Resident, or Naturalization, status.

18. In addition, about nine of these authorised Immigration Officers are required to record and monitor all passengers' arrival/departure information, in OTRCIS. The type of information that is inserted into OTRCIS include: travelling document details; length of stay; and the type of access in/out of Montserrat. The department utilises this information mainly for Intelligence purposes.

[5] *Executive Summary, Montserrat Integrated Border Security Unit (IBSU) Operational Report (Feb. 2013 to Oct. 2017) and Recommendations for Way Forward - October 10, 2017, MCRS/RMPS, Government of Montserrat.*

CHAPTER 3 OUTSOURCING

Service Level Agreements and Contracts

20. **OTRCIS Master License Agreement**. In regards to SLAs and contracts, it was noted that neither Montserrat, nor the other COTs that use OTRCIS, have physically signed a contract or agreement with initially with MEMEX or SAS. The overseas System Administrator (SA) in Miami is the person who signs the annual contract on behalf of all the COTs; therefore, the RMPS is unaware of the terms and conditions of the Master License Agreement.

21. **Cloud Hosting Contract.** In March 2019, the RMPS signed a three-year, non-cancellable, *Novation Agreement* with the Foreign Commonwealth Office-Overseas Territories Dependencies (FCO-OTD) Criminal Justice Office in Miami, and the SAS Software Limited in the UK, to switch over to Cloud Hosting. This agreement is a supplemental document to the Master License Agreement, and it outlines the terms and conditions pertaining to the Cloud Hosting services, the scope, usage, warranties, fees and payment, access rights, change management, technical support, security, ownership, intellectual property rights, confidentiality, data protection, termination/expiration, and so on.

22. **Access and Usage.** There are rules in the *Novation Agreement* that covers the users' access to, and use of, the Cloud Hosting system. The RMPS's service provider is also included as they will have authorised access to the OTRCIS Cloud. The rules cover matters such as:

- approved communications link, technology or hardware required for the Cloud hosted system to operate properly
- who can access the OTRCIS Cloud
- change request process
- usage and prohibited activities
- provision of customer materials (software and/or data licenses)
- customer's service provider

23. **Compliance and Virus Warranties.** The RMPS is liable for ensuring that the publication, transmission, and receipt of all of the organisation's material is in compliance with all applicable local, state, and federal laws, and regulations; especially for property rights, defamation, consumer protection, personal privacy, and false or deceptive trade practices. In addition, the RMPS has to ensure that OTRCIS will not be infected by viruses, due to RMPS materials or otherwise.

24. **Data Security and Protection.** The Cloud Hosted system will be managed by the SAS Institute Inc. based in USA; and users will access OTRCIS via the *SAS Memex Platform v 2.23*. SAS will implement and maintain the following technical and organisational security measures:

- 24/7 IT systems monitoring;
- infrastructure for hosting services including hardware, network and UPS protection, data quality floor space;
- environment, including air conditioning and fire suppression;
- physical and logical security;

- operating systems updates;
- regularly-scheduled back-ups to be used for recovery purposes;
- technical support;
- authenticated and authorised users access privileges to the OTRCIS Cloud;
- SAS software and 3rd party products administration, including installation of new releases of SAS software, and application of hot fixes;
- service level warranty
- annual audits, and global network penetration tests to include changed production apps exposed to the Internet;
- Cloud hosting System Administrator authorisation and server authentication to protect data transfers; and
- server authentication for external facing, via the use of digital certificates from reputable certifying authorities.

SAS has the legal right to terminate or limit the use of the Cloud Hosted system without giving prior notice, in the event of any unauthorised access to, or use of, the OTRCIS Cloud.

25. All the personal data received by SAS in respect to the Cloud Hosting services (i.e. RMPS material and users), SAS will (i) only use the personal data for purpose of providing the hosting services; (ii) implement and maintain technical and organisational security measures against unauthorised access, use, or modification, destruction, or disclosure; (iii) comply with SAS Solutions OnDemand and Business Customer Privacy Policy.

26. In addition, neither RMPS users nor SAS, can give out or share user access rights details or permission to access to OTRCIS software; the stored data; and OTRCIS documentation; to any unauthorised 3rd party or entity. Should the *Novation Agreement* be terminated, both the RMPS and SAS are obligated not to disclose any confidential information that was received under the Agreement to any third party for the duration of five (5) years, unless advanced written authorisation is given.[6]

Ownership and Data Rights

27. SAS owns the OTRCIS software; however, each COT/BOT can make copies only for disaster recovery and back-up purpose. The information that is inputted into OTRCIS by the COTs is owned by them; therefore, neither party can delete, obscure, or modify the other party's proprietary rights notices.

Intellectual Property

28. Only RMPS authorised users have the right to access and use OTRCIS from and within the Territory, including any documentation provided by SAS, for Police intelligence operations. SAS can use the material provided by RMPS (i.e. permitted data, authentication credentials, software, and other materials) and marks (i.e. trademark, service marks, or trade names that are reproduced or displayed in OTRCIS) for the purpose of performing the Cloud hosting services.

[6] *SAS Novation Agreement, 05 March 2019*

CHAPTER 4 INFORMATION TECHNOLOGY OPERATIONS

Problem and Incident Management

29. Currently, the local SA refers any problem that arises with OTRCIS, to the Miami-based SA. However, for Cloud Hosting, the *Novation Agreement* states that SAS will provide support from a technical support centre closest to the country where the software is installed or where the users reside. The contractor can also refer certain issues to other SAS technical support centres.

30. In the *Novation Agreement*, SAS warrants that the Cloud Hosting system will not experience more than the maximum monthly downtime of seven (7) hours; and 3-day prior notification of any planned outage for maintenance.

Change Management

31. As per the *Novation Agreement*, the RMPS can request in writing any changes or modifications to be made to the components of the Cloud hosted system or services, for an additional fee. SAS will follow a strict change control process that will ensure all the changes effected, will be accurately documented.

CHAPTER 5 INFORMATION SECURITY

Human Resources Security

32. **Recruiting and Employment.** The RMPS Organisational Chart includes a Human Resource (HR) section that employs and manages Officers; but the GoM Human Resources Management Unit (HRMU) is responsible for recruiting the administrative staff. However, the RMPS thoroughly vets all Police recruits, Custodian staff, and the potential Administrative personnel, before they are hired. It is the standard practice for RMPS's staff to be employed on a long-term basis.

33. **Segregation of Duty.** There is not much segregation of duty in policing operations, as the majority of RMPS Officers perform dual, triple, and sometimes quadruple job functions. For example, some Inspectors and the Deputy COP have oversight of more than one department; Immigration and Customs Officers are also Special Constables; the local OTRCIS SA also performs IT, HR, Digital Forensics, and Interpol Intelligence duties.

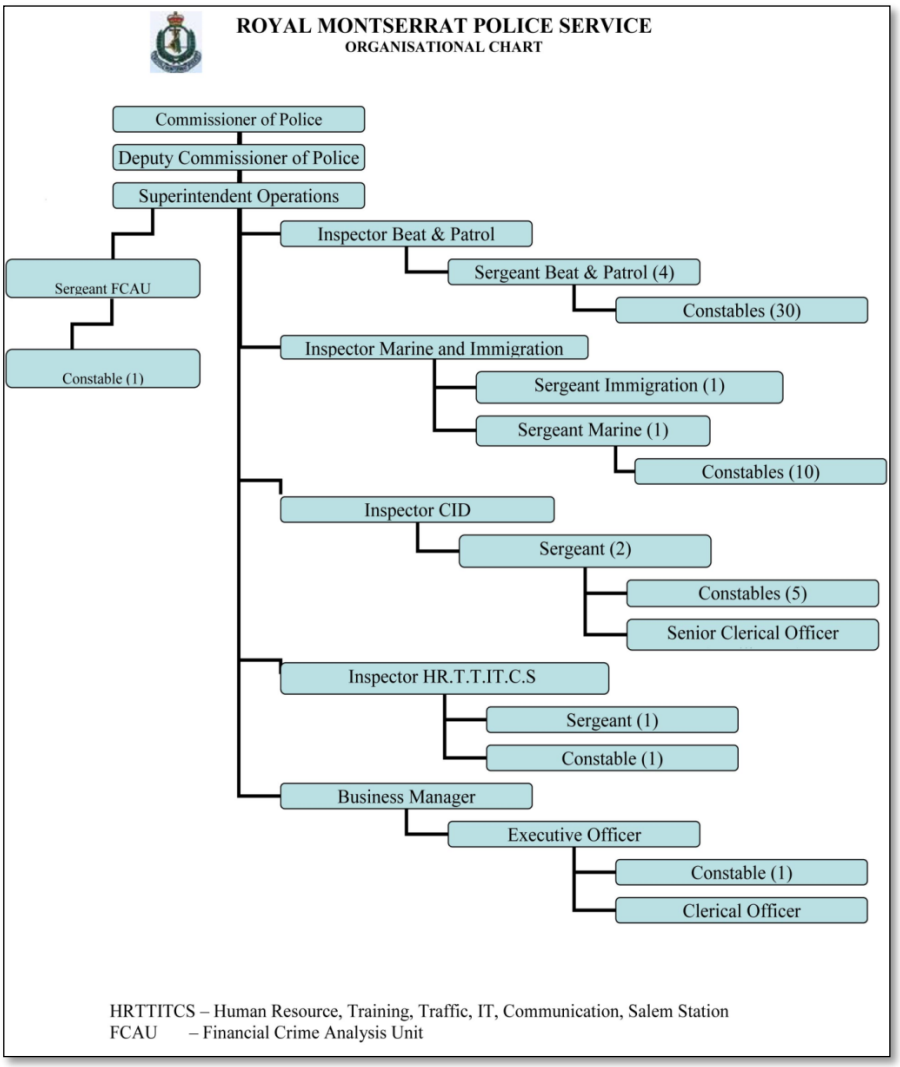


Figure A - RMPS Organisational Chart

34. The overlapping of job roles is not ideal and would normally be a great cause for concern in mainstream organisations, due to the risk of fraud and malicious acts such as sabotage and collusion between employees. However, because the culture of the RMPS is to uphold and enforce the laws of the land, a high level of confidentiality is involved. Therefore, job rotation and cross training of more than one individual is advantageous because this will:

(i) provide additional control in reducing risk of fraudulent or malicious behaviour; and/or

(ii) decrease dependence on a single employee.

35. There is clear segregation of duty in the oversight of OTRCIS. The Miami-based SA has the executive authority to approve and carry-out key administrative, technical and support duties. The local SA has limited influence, and has to obtain authorisation from the Overseas SA to execute most tasks as summarised below:

Overseas System Administrator	RMPS System Administrator
• sign annual Master Agreement on behalf of all the COTs.	• create customised OTRCIS forms (for the benefit of Montserrat OTRCIS users only) and resolve any issues with the forms.
• implement changes to the OTRCIS system.	• delete errors, duplicate forms, and user accounts (if authorised by Overseas SA)
• conduct remote network and server maintenance	• create Covert folders
• provide helpdesk support	• unblock user accounts.
• perform daily backups of the OTRCIS data.	• train new OTRCIS users.
• monitor and protect the network against internal and external malicious attacks	• generate audit reports for court purposes, once requested by a Magistrate, Judge, or Lawyer
• provide requested historical user account information (audit trails)	• generate monthly RMPS statistical reports
• conduct security investigations (on request)	• liaise with Overseas SA
• manage user accounts: – creation of user accounts – generate, issue, and change passwords – removal of user rights and permissions – deactivation and unlocking of user accounts; etc.	
• liaise with and supervise local COT's System Administrators	
• other	

36. **Confidentiality.** RMPS Police Officers do not sign the *GoM's Oath of Secrecy*, which is a HRMU's requirement. When new Police Officers are sworn in, confidentiality is covered in the *Police Oath*, where they pledge to carry out their duties according to the laws of Montserrat.

The directives in reference, are listed below in Figure B, from Section 54, Part 2, Offenses and Discipline, 6(f) (i) - (v) of the *CAP 10.01 Police Regulations*. The *Police Oath* is signed by the officers and placed on their personnel file. The Financial Crime Analysis Unit team has the added security procedure, of undergoing Polygraph testing.

> *(f)* breach of confidence, that is to say, if any officer—
>
> (i) divulges any matter which it is his duty to keep secret; or
>
> (ii) gives notice, directly or indirectly, to any person against whom any warrant or summons has been or is about to be issued, except in the lawful execution of such warrant or service of such summons; or
>
> (iii) without proper authority communicates to the public press, or to any unauthorised person, any matter connected with the Service; or
>
> (iv) without proper authority shows to any person outside the Service any book or printed document the property of the police authorities; or
>
> (v) makes any anonymous communication to the Commissioner of Police or any other superior officer;

Figure B - Offenses and Discipline Extract from CAP 10.01 Police Regulations

37. However, it is mandatory for newly appointed Customs Officers to sign the *Oath of Secrecy*, which is a compilation of extracts from Section 2 of the *Official Secrets Acts* of 1911 (as amended in 1920); and Section 1(2) of the *Official Secrets Act*, 1920. This document outlines and discourages the unlawful communication, retention, use of, and improper protection of GoM's confidential documentation, information, and passwords.

38. The OAG noted that of recent, newly appointed Immigration Officers are also required to sign the *Oath of Secrecy*.

Physical Access Controls

39. **Visitors.** The RMPS have very stringent Physical Access Controls in place that restricts unauthorised access to controlled areas or facilities inside the Brades Police Station; all RMPS staff and visitors have to adhere to these rules. Visitors to the Police Station must report to the Reception Desk (Enquiries) and the Duty Officer will notify the relevant RMPS staff that they have a guest. Visitors are not required to sign in/out, nor issued visitors' ID badges; they must, however, be accompanied in and around the building and compound, at all times, by either the individual they came to see or by an assigned escort.

40. **Custodian Personnel.** The custodian staffs are placed on a very strict cleaning roster. They are restricted to performing their duties between the hours of 6:00 am - 2:00 pm, when there will be a high volume of activity and personnel, in the building.

41. **Security Mirror.** In the Reception Lobby, a round mirror is mounted high on the opposite wall and angled to face the front desk. This mirror enables the Duty Officers to view and monitor the flow of human traffic coming in and going out of the door leading into the office areas, and from lobby restrooms, behind the partitioning wall.

Figure C - Security Mirror in Reception Lobby

42. **Server Room.** The RMPS has its own Server Room at the Brades Police HQ; it is a centrally located windowless room, with solid concrete ceiling and walls. Only three (3) people are authorised to enter the Server Room, they are the Commissioner of Police (COP), Deputy COP, and the RMPS's OTRCIS System Administrator (SA). The COP and the SA are the only two persons who have keys to the Server Room; however, the Deputy COP can retrieve the key if the COP is absent. Custodian staffs are not permitted to enter this room; and unauthorised personnel have to be granted permission by the COP, to access the Server Room.

43. **IT Room**. The IT Room is a regular office with windows that are not weatherized or impact resistant; however they are protected from direct sunlight and unlawful access by a lowered, external, metal Bahama (or Bermuda) hurricane shutter. The door to the IT Room is locked with a key and apart from the SA, only the Deputy COP has a copy. Persons, that need to go into the IT Room, have to be granted permission by the SA who has to be present at all times.

Environmental Security

44. **Backup Power Supply.** The RMPS is connected to the GoM Headquarters communal auxiliary generator in Brades. The Salem Police Station does not have a backup generator. In addition, there is a twelve (12) battery Uninterruptible Power Supply (UPS) tower, in the RMPS's Server Room, all of the 110 volts electrical outlets throughout the Police Station, are connected to it. In the event of a power outage, sufficient power is provided to allow RMPS staffs to back up their data and perform orderly shut-down of their computers.

45. **Manual Bypass Switch.** There is a manual bypass switch mounted on the wall in the Server Room for occasions when the Tower UPS has to be serviced and maintained, on site, without the risk of disruption in power, and for the maintenance person's safety.[7] The load for

[7] *https://www.ecopowersupplies.com/ups-maintenance-bypass-switches*

the 110 voltage electrical sockets will be switched over to the main power source provided by Montserrat Utilities Limited (MUL).

46. **Circuit Box Safety Switch.** The circuit breaker box in the Server Room has a safety switch (lever) to quickly and completely shut down the circuit breaker panel in the event of an emergency situation, in the Server Room; for example an electrical fire.

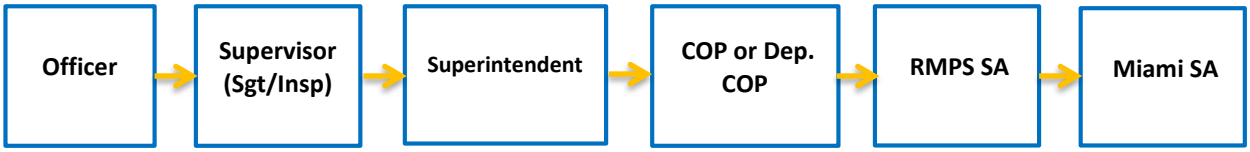
Figures D & E - RMPS Server Room 12-battery UPS Tower and Circuit Box with Metallic Emergency Safety Switch

47. **Fire Extinguishers.** There is only one (1) dry powder fire extinguisher mounted on the wall in the corridor of the Sensitive Crime, wing. At the time of the walk-through, it was noted that the fire extinguisher was last tested in May 2018.

48. **Air-Conditioning.** Both the IT and Server Rooms are air-conditioned in order to keep the OTRCIS-related computer and network equipment cool. The temperature in the Server Room is fixed at 69^{o} Fahrenheit; whereas the temperature in the IT Room is regularized between 61^{o} - 64^{o} Fahrenheit (61^{o} F being the lowest setting), depending on the time of the year and the external temperature.

Logical Access Controls.

49. **Authorisation Chain of Command.** It is mandatory that permission is sought and granted before some OTRCIS-related tasks are executed. The COP (or Dep. COP) has to make the final decision and give his authorisation. Formal requests have to be sent via email from the requesting Officer to their immediate Supervisor for the first round of approval; this approval process will continue up the RMPS's chain of command until the request reaches the COP for sanctioning. After full authorisation is given, the request is to the RMPS's SA who re-directs the email to the Overseas SA, to actuate the request. For example, the generation of User IDs and passwords.



Flow Chart A - RMPS Chain of Command

50. **Internet Usage Policy and Agreement.** The COP approves and determines the levels of Internet access and usage restrictions for Police and Immigration Officers only. The MCD's Head of Department is responsible for deciding for Customs Officers. Officers are required to read the *Government of Montserrat's Internet Policy,* and sign the *Internet User Agreement*, before Internet access is granted by DITES.

51. **Creation of User Accounts.** The Superintendent (Supt.) of Police, who is the Head of Operations, is the person responsible for sending the list of new Officers to the COP for sanctioning. The email contains the (i) name of the Officer, (ii) rank, and (iii) user role, in order to create new user accounts; an unlimited number of user accounts can be created.

52. **Deactivation of User Accounts & Removal of User Rights and Privileges.** When RMPS Officers leave or are transferred, the protocol is for the Supt. to email the COP a list of these officers requesting that their accounts be deactivated, or certain user rights/privileges be restricted. The COP will give his consent and send the request to the local SA, who in turn forwards it to the Miami-based SA to action.

53. **User IDs and Passwords.** Unique User IDs are generated by the Overseas SA and emailed to the local SA for distribution. These IDs contain each COT country's identifying letters and a number, which will forever be associated with an Officer (Police, Immigration, and Customs) and their user account. These User IDs are always eight (8) characters in length; therefore, as the numerals increase, the number of letters will decrease; for example:

- **MONTSR** 67
- **MONTS** 484
- **MONT** 1052

54. OTRCIS Passwords have a minimum of 8 alphanumeric characters and linked to each user account and its assigned User ID. They are created by the Miami-based SA, who personally calls each of the new users to give them their password. Passwords cannot be changed by the users themselves, a formal request has to be sent to the Overseas SA to effect a change. A log is kept of all the passwords that were changed and the password file is encrypted for added protection.

55. **Role-Based Access Control.** OTRCIS utilises Role-Based Access Control (RBAC) Security groups to manage access control to folders and files. Collections of user accounts are grouped together according to their specific job tasks, and are assigned user rights and permissions to gain access the allocated OTRCIS folders. For example, all Police Officers can view and access all OTRCIS folders and related forms (files), except for Covert folders; whereas, the Immigration and Customs Officers are restricted to viewing and accessing only four (4) folders which pertains to their job functions. They are not allowed to see or access Covert files unless required to.

56. It is also a policy that different ranking Officers will have different levels of access to OTRCIS and it is the COP who determines this. For example, the authorised Senior Customs Officer can access, track, and utilise the OTRCIS data for intelligence purposes, but Junior Officers are limited to inserting the passengers' travel document and journey details, into the forms.

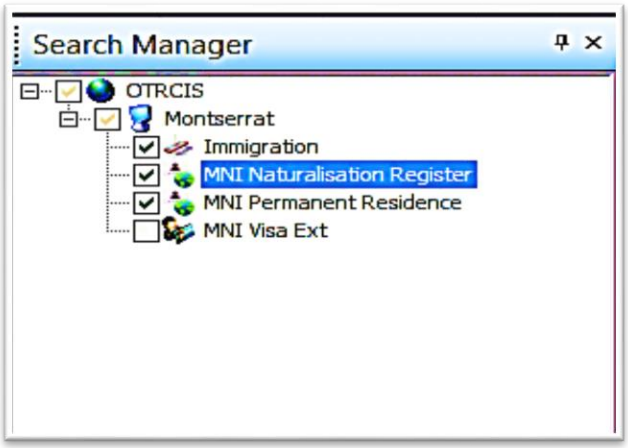


Figure F - Immigration Dept. & Customs Division Security Group Folders

57. **Covert Folder and Files.** Covert folders are secret folders that contain confidential case file(s), and they cannot be opened by unauthorised users unless they were assigned to have access privileges to the folder. Therefore, when a reported crime under investigation is deemed highly sensitive, and the Officer presiding over the case does not want the information to be divulged, he or she can request that the sensitive case file(s) be concealed in a Covert folder. A request is sent by email to RMPS's SA to create the Covert folder for the case file(s) and give access to a specified number of persons; if any. The information provided in the email includes the:

- name the Covert folder is to be given;
- sensitive case file's Unique Reference Number (URN); and
- name(s) of the officer(s) who can access the Covert folder and case file(s).

58. The SA first verifies if the case file is the correct one before logging into the server and creating the Covert folder; the case file's URN is then copied and inserted into the newly created Covert folder; and access rights and privileges are assigned to the specified person(s). It is important to note however, that the SA cannot access Covert folders, unless he is one of the assigned individuals authorised to access sensitive case file(s).

59. **User Account Blocking and Time-Outs.** User will be 'blocked' (i.e. locked out) from their accounts after three (3) incorrect log-in attempts. They will not be able gain access to their account until it is unblocked by the Overseas SA or the local SA. Similarly, user accounts are set to automatically log-off when there is no activity for over 20 to 30 minutes; the user will have to log back into OTRCIS. The Overseas SA is responsible for setting the time-out period.

60. **Temporary User Accounts.** Temporary user accounts are sometime created for visiting overseas Law Enforcement and support staff; these accounts are created as per the users' job functions or tasks to be performed. These accounts have a set expiration date and time, and will automatically deactivate, when the set time period ends.

61. **Encryption.** The encryption method used by OTRCIS to protect the data stored on the server and transmitted across the network via the Internet, is RSA Cryptography; it was developed by the intelligence and security organisation, Government Communications Headquarters (GCHQ).

62. **Audit Logs.** Audit logs or trails, are created and stored on the server for all OTRCIS user account activities; from the time the user logs-in, every key stroke and mouse click is recorded. These user account historical records span from the inception date of when each COT started using OTRCIS. If the RMPS suspects an Officer of breaching, any of the *Offenses and Discipline* terms outlined in the *CAP 10.01 Police Regulations;* the COP can make an official request to the SA for a copy of the suspect's user account audit trail. If the suspect(s) audit logs confirm illicit activity, the suspect's user account is disabled and an investigation is conducted. The RMPS's SA can run basic audit trail reports that will include the following particulars. If a more detailed report is required, the SA in Miami will provide one.

63. **Remote Access.** Only the Miami-based SA has the authorisation to remotely access the OTRCIS server and the RMPS users' personal computers, for maintenance and troubleshooting purposes.

64. **Cloud User Accounts.** The COP indicated that a few months prior to this audit, the RMPS had just recently signed an agreement with the OTRCIS contractor SAS, to switch over to Cloud hosted servers. With the Cloud hosting system there will be enhanced security features such as the automatic deactivation of user accounts once there is no activity for three months; and users will have the autonomy of periodically changing their own passwords.

Communications and Operations Management

65. **OTRCIS Security Operating Procedures.** The contractor disseminates a mandatory document called the *OTRCIS-CIM Security Operating Procedure* (SOP) to all the COTs for their users to read and sign. This recent SOP document outlines what is expected of OTRCIS users, in regards to:

- Data Security, Legal mandates, Territorial and International Laws
- IT Security incidents
- Data Transfer, Viruses, Unauthorised software and the unlawful distribution of OTRCIS and associated data
- Hardware maintenance, Software issues, and system Change Authorisation
- Logical and Physical Access security
- Email usage protocols
- Data ownership

66. **Network Security.** The RMPS Server Room only houses minimal pieces of network equipment such as the heavy duty backup power supply; two (2) network switches; and a service provider router for Internet connection. The RMPS's SA maintains them with the assistance of the overseas SA. DITES only hosts the physical OTRCIS server; it is only responsible for ensuring that there is a steady, reliable, source of power to maintain the network link that connects RMPS to the server, and to secure the server in inclement weather or in an

emergency. DITES server room personnel cannot gain access to the data stored on the server, only the SA in Miami is authorised to access and perform administrative, defensive, and maintenance tasks to the server, via remote access.

67. The OTRCIS system network is protected by various firewalls and other network monitoring tools to detect and prevent internal or external unauthorised access, or malicious attacks; and to inhibit the spread of computer viruses.

CHAPTER 6 APPLICATION CONTROLS

Input and Processing Controls

68. **Training.** Before new user accounts can be created, it is mandatory that the local SA train all new users on how to navigate and use the application forms, utilising the Memex *Data Input Standards* to:

- Format the information being inserted into the forms (for e.g. capital letters; no punctuation; passport, telephone, D.O.B., time, and date format; no spaces; etc.)
- Perform various Searches, and to manipulate and view results
- Sort information and Print
- Enter and update a record

69. After the training is completed, new user accounts are requested and created before the local SA emails a link to each new user to download a copy of the OTRCIS web 'client' from the server. It is important to note that OTRCIS is not installed directly on the user's personal computer (PC) but into a *Temporary* folder under the user's account. Therefore, users will not be able to access their OTRCIS account, if they try to log into OTRCIS from another computer.

70. **Controlled Use of OTRCIS Forms and System.** The OTRCIS forms are utilised mainly for the recording of annual leave (for Police only); Immigration matters; general incidents; crimes that occurred in Montserrat; and other police intelligence matters. Currently, there are one hundred and ten (110) OTRCIS forms, of which only sixty-four (64) are used by Montserrat; some of these forms were customised by the local SA to incorporate criteria specific to the island. These modified forms can only be used by the RMPS, Customs, and Immigration divisions. Lower level Customs Officers are restricted to just inserting travellers' personal and journey details into the forms; and only certain senior ranking Officers have the authority to access to, can manipulate and utilise, the information.

71. Another noted control measure, as per the *Novation Agreement* is that the total number of authorised users, who can be logged-in to OTRCIS system at one time, is only forty-five (45).

72. **User Interface.** OTRCIS forms have a similar design to an Excel worksheet where one form can have several tabs to enable users to switch between the different sub-forms, located in the master form. The forms are designed with several Graphical User Interface (GUI) input control features such as:

- contained, radio, and theming buttons;
- input text fields;
- date pickers;
- check boxes;
- list menus;

for the accurate, reliable, complete selection, insertion, and appending of information.

73. **Saving and Editing Forms.** For new OTRCIS forms there are compulsory fields are highlighted in red that must be filled. The system will not allow the forms to be saved, unless these required fields are completed and the users click the 'Append' button. Once saved, the

system automatically locks the forms. Therefore, if information has to be amended, the forms have to be unlocked with the 'Unlock' button, and the changes are saved via the 'Update' button. All activities executed in the forms and the persons who performed these actions, are logged by the system via their User IDs.

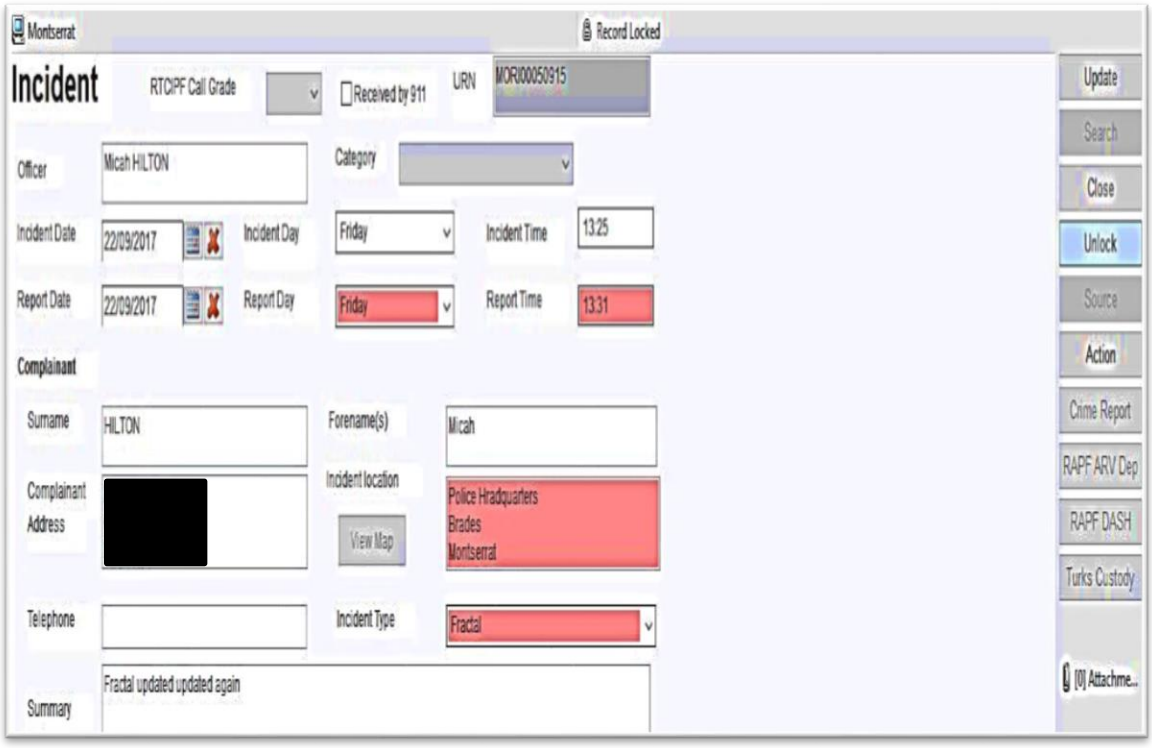


Figure H - Example of OTRCIS Form Input and Modification Controls

74. **Timestamps.** When reported crimes or incidents are inserted into the forms and saved, the system automatically timestamps (date & time) the files. Therefore, if a user goes back and amends or tries to falsify information in a form, the system will not change the timestamp to when the information was modified; it will still retain the original date and time when the file was created.

75. **Calendars and Date Format.** The current date can be inserted into the OTRCIS forms either manually or via an embedded date picker (calendar). The date format of the calendar is British and corresponds to the OTRCIS server's date and time; therefore, if an American date format is typed in, the system will automatically change it. In addition, if the current date is inserted using the embedded calendar, the user will not be able to change it manually.

76. **Error Alerts and User Prompts.** Whenever there are errors in the forms, the system is set up to alert users with various types of error messages, depending on the error. For example, if the incorrect date was inserted an error message window will appear. The system will also prompt users to perform certain actions or tasks with messages in red letterings as shown below in *Figure I*:

Figure I - Example of OTRCIS Form Input and Modification Controls

77. **Flags and Interest Markers.** The OTRCIS system enables users to set two types of notification indicators:

- A **Flag** for when errors are found in forms; the reviewer can point out the mistakes and give instructions for corrections, by typing annotations in the **Contact** or **Message** fields.
- **Interest Markers** to notify Officers when certain information of interest is recorded in the forms; for example, Immigration or Customs Officers can set an interest marker when they want to monitor the movements of specific person(s) coming in and going out of Montserrat.

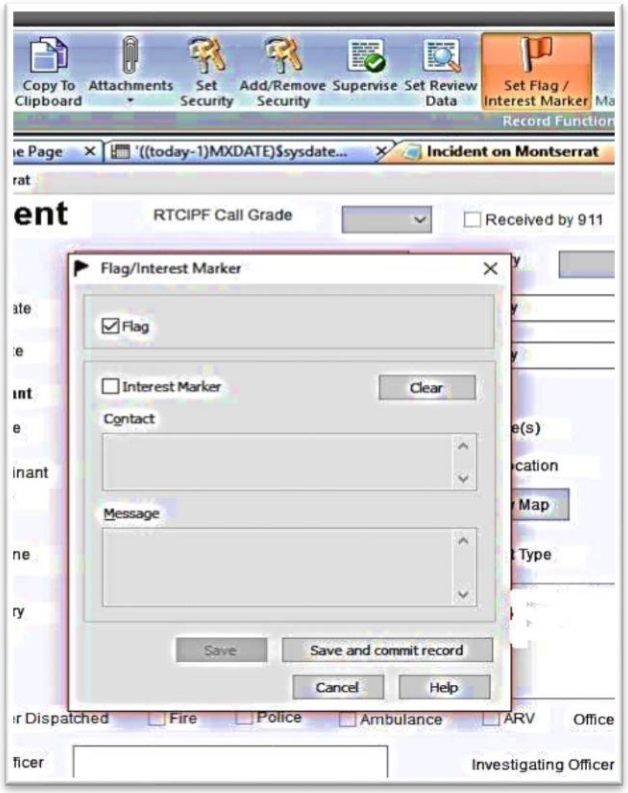


Figure J - Flag/Interest Marker

78. **2-Tiered Authorisation and Security Group Privileges.** The OTRCIS Annual Leave Form is designed with 2-tiers of approval. Once an Officer submits a leave form, for whatever reason (vacation, compassionate leave, study leave, special leave, and lieu leave) at Level 2, the form has to be filled out by Supervisors, and then it is forwarded to Level 3 to the Supt. or other higher ranking Officers.

79. Another security feature in the Annual Leave Forms is that drop down menus at each level, will not be visible to click on unless Officers are directly assigned to either privilege group; i.e. Supervisor or Senior Officer.

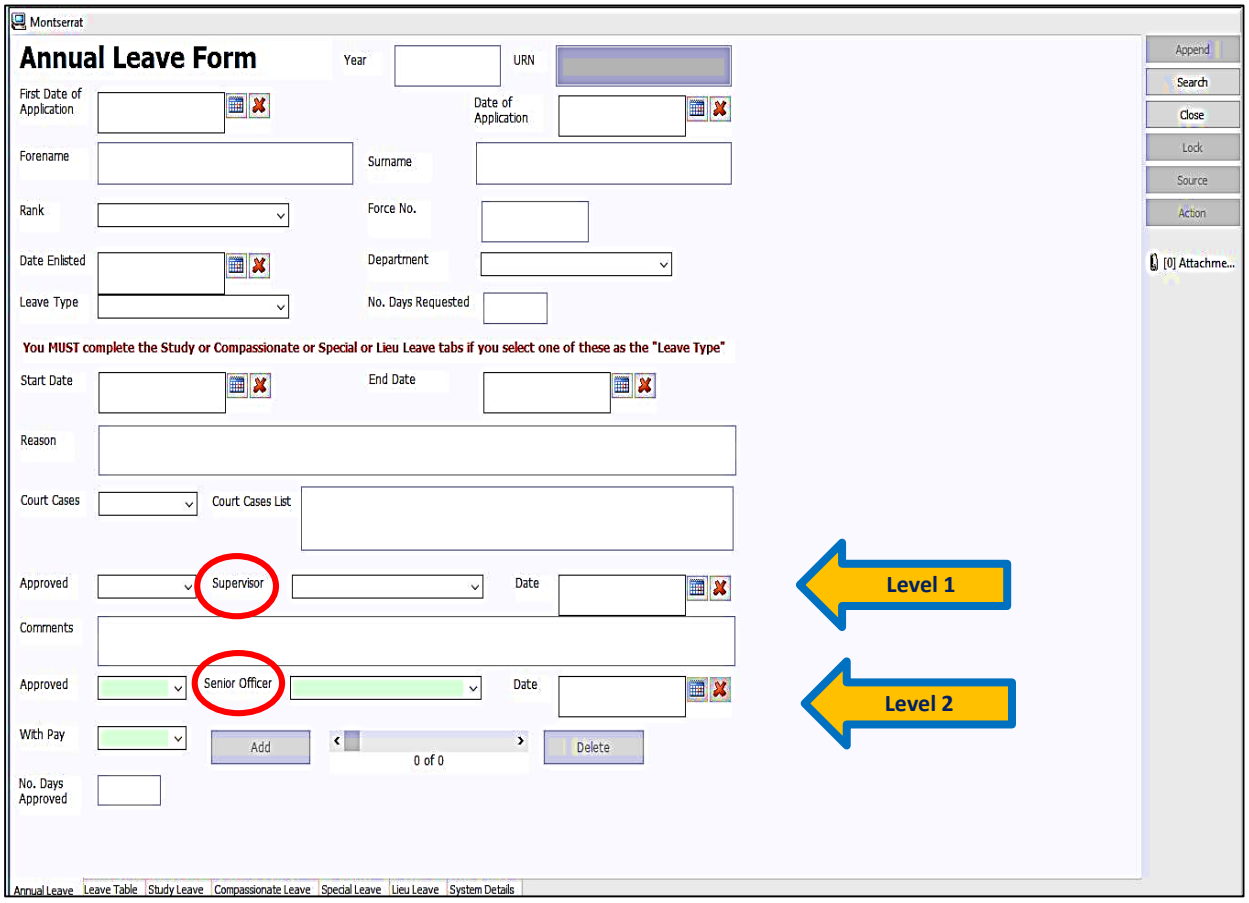


Figure K - 2-Tier Authorisation

Output Controls

80. The RMPS have access to and can conduct searches, in all of the COTs and BOTs databases in Read-Only mode; but the Police Officers are unable to extract and print any information. However, in regards to Montserrat's OTRCIS data, if hard copies are required an official request has to be sent along the ranks to the Supt. or COP to sanction the request. Once approved, all requests are forwarded to the RMPS's SA who extracts the data and prints the reports; but if the task is beyond his scope, the request will be forwarded to the SA in Miami.

CHAPTER 7 DISASTER RECOVERY AND BUSINESS CONTINUITY

Disaster Preparedness Plan

81. In 2015, the RMPS in conjunction with the Montserrat Fire and Rescue Service (MFRS), introduced a comprehensive document called the National Disaster Plan (NDP), which replaced their annual Hurricane Plan. This newest plan details the pre- and post- disaster training, preparedness, and operations activities for each Unit; and specifies who the designated support personnel are, and their roles, in times of disaster. It is updated annually, and was created in accordance with the *CAP 10.08 Emergency Powers Act.*[8]

82. However, in keeping with the context of this IS audit, the disaster plan clearly outlines the course of action to be taken for the safety and security of all the buildings and equipment that the RMPS owns, or is responsible for. In addition, the RMPS has a dedicated safe room for the storage of their computer-related assets, in the event of inclement weather; this is a solid concrete room with a double concrete roof. They do not secure the OTRICS server as DITES is responsible for safeguarding all equipment housed in their Server Room.

Backup and Recovery

83. In the aftermath of natural disasters, or other crisis situations, the MEMEX/SAS datacentre in Miami performs daily automatic back-ups of all OTRCIS data on their servers, from their end in Miami to ensure that there can be full recovery and resumption of the OTRCIS system. The backed-up information extends as far back as 1996, when the software was first launched. The individual COTs are also responsible for the frequent backing-up of the OTRCIS data stored on their servers.

[8] *Royal Montserrat Police Service and Montserrat Fire and Rescue Service National Disaster Plan 2015/18*

CHAPTER 8 FINDINGS AND RECOMMENDATIONS

Findings

84. **Non-operational Door Access Control and External Surveillance Camera Systems.** The Brades Police Headquarters had a buzzer door system for controlling the traffic in and out of office areas, and an external security camera system, which has been non-operational for several years. The COP indicated that he has put forward business cases for the upgrade and/or replacement of these defunct security systems some years ago.

Figure L - Non-operational External Security Cameras

85. **Redundant Emergency System.** The Brades Police Station is outfitted with a non-operational Emergency System (ES) comprised of fire alarms, smoke detectors, and temporary lock-up (or jail) cell buzzers. Reportedly, the jail cell buzzers malfunctioned and triggered off the other alarms; therefore the control panel was disconnected by the vendor. The ES has been disengaged for approximately three to four years.

86. **Inadequate Fire Suppression Equipment.** The walk-through inspection of the main foyer area showed evidence that a fire extinguisher was mounted on the wall; there is uncertainty when and why it was removed, and if it will be replaced. Inspection of the IT and Server Rooms, revealed that there are no electrical fire extinguishers installed in either of these locations.

87. **No Auxiliary backup power supply and proper surge protection.** Salem Police Station is not equipped with a heavy duty UPS, nor is it connected to an auxiliary generator as backup sources of power for their computers and other electrical office equipment. At one time, all of the computers were plugged into interactive line UPSs before the batteries died; therefore, they are not protected from power surges. Secondly, if information was being input into the OTRCIS forms at the time of a power outage, it would be lost and would have to be inserted again when the electricity was restored. The local SA has indicated that the RMPS has future plans to install a backup generator at the Salem Police Station, and replace the inoperative line interactive UPSs.

88. It was also revealed that the Brades Police Station used to have its own backup generator, which was removed and the organisation linked to the Brades Headquarters' communal generator instead.

89. **Sensitive Crime Wing.** Access to the Sensitive Crime offices and IT room, is usually controlled by a closed door with a keypad lock. However, it was noted that the door was being left open, because the keypad battery needed to be replaced.

Recommendations

90. **Door Access Control and Surveillance Cameras Systems**. We are recommending that the Head of the RMPS renew their effort of attaining replacements for the non-operational front buzzer door and external security camera systems. The new door access control system could be keycard based that generates audit trails of authorised traffic of access to the building. Alternately, the RMPS can consider procuring a keycard door access control system combined with both internal and external camera surveillance. Another option is a biometric security system that utilises devices such as fingerprint or hand geometry readers, or facial recognition scanners.

91. **Environmental Control Equipment and Emergency System**. Environmental controls can prevent or mitigate potential damage to facilities, interruptions in service, and can potentially save lives. Therefore, we are strongly advising that fire extinguishers be installed in the Server and IT Rooms, and in the foyer at the Brades Police Station. It is also recommended that a more effectual Emergency System is reinstated for the early detection and warning for smoke and fire; as well as to facilitate distress calls from the jail cells.

CHAPTER 9 CONCLUSION

92. The Office of the Auditor General (OAG) has established from the findings of this IS Audit that the OTRCIS software is a very robust application and that the related computer and communication systems (internal and external), are properly secured against unauthorised access and modification of information and denial of service attacks. This has been achieved by means of very stringent Outsourcing, IT Operations, Application, Information Security, Disaster Recovery and Business Continuity controls, policies, and procedures that were instituted by both the contractor and the RMPS.

93. The weaknesses detected were Environmental and Physical Access related, and it is in the best interest of the RMPS to consider and address the shortcomings and recommendations that were highlighted, in a timely manner.

CHAPTER 9 MANAGEMENT RESPONSES

An exit meeting was held with the Commissioner of Police and a draft report shared to solicit a Management Response to findings/observations and recommendations.

In his response the Commissioner of Police stated that he had “read the Report and is satisfied with, the contents and findings of the report; including the agreed upon additional information and recommendations discussed in the Exit Meeting”.

REFERENCES

Websites

https://1997-2001.state.gov/global/narcotics_law/1998_narc_report/eastcarib98.html

https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Memex_Technology_Limited.html

https://web.archive.org/web/20110426124243/http://www.sas.com/news/preleases/Memex.html

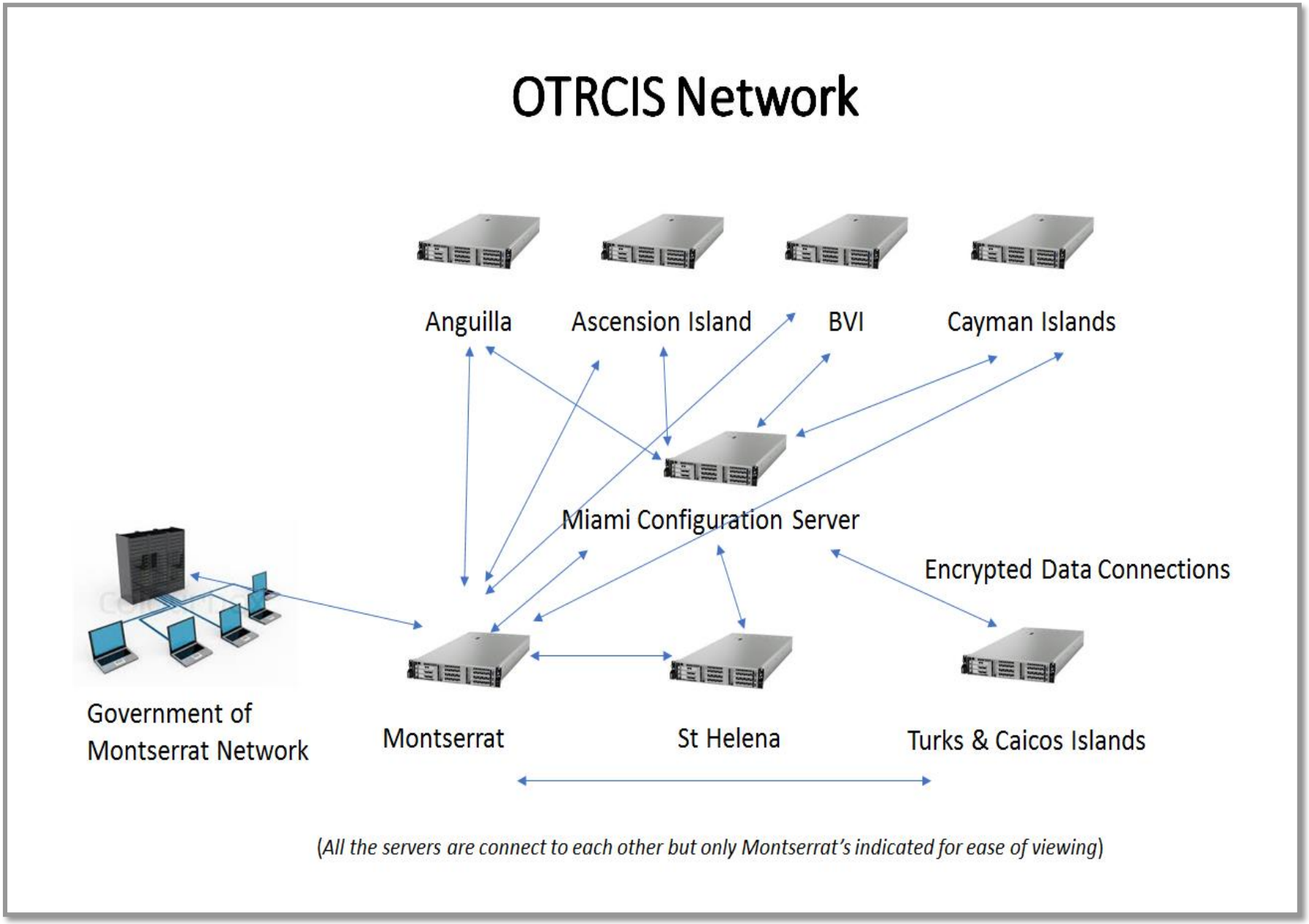
https://www.theyworkforyou.com/wrans/?id=2009-06-16c.279058.h

Books

INTOSAI WGITA IDI Handbook, IT Audit for Supreme Audit Institutions, February 2014

APPENDICES

APPENDIX I - OTRCIS Network Diagram



APPENDIX II - OTRCIS Client, Installation, and Login Windows

Follow these instructions to install the New OTRCIS Client.

This is a two step process.

Step One

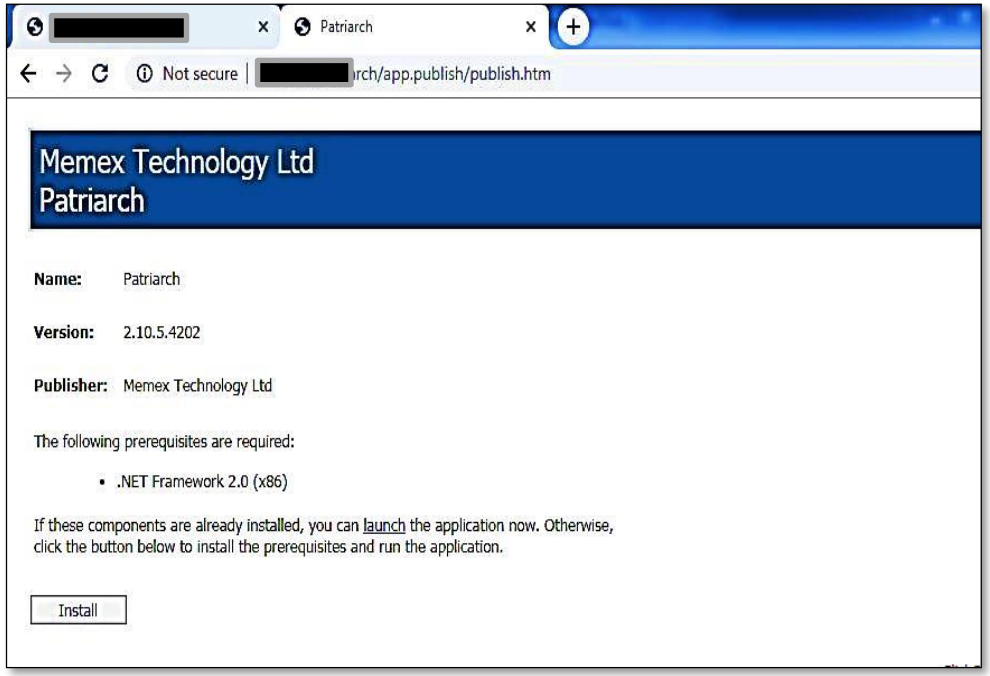
- Click here to uninstall the old OTRCIS Client
- When prompted, Click on "Run" to execute
- Once it is successfully uninstalled, click on "OK"

Step Two

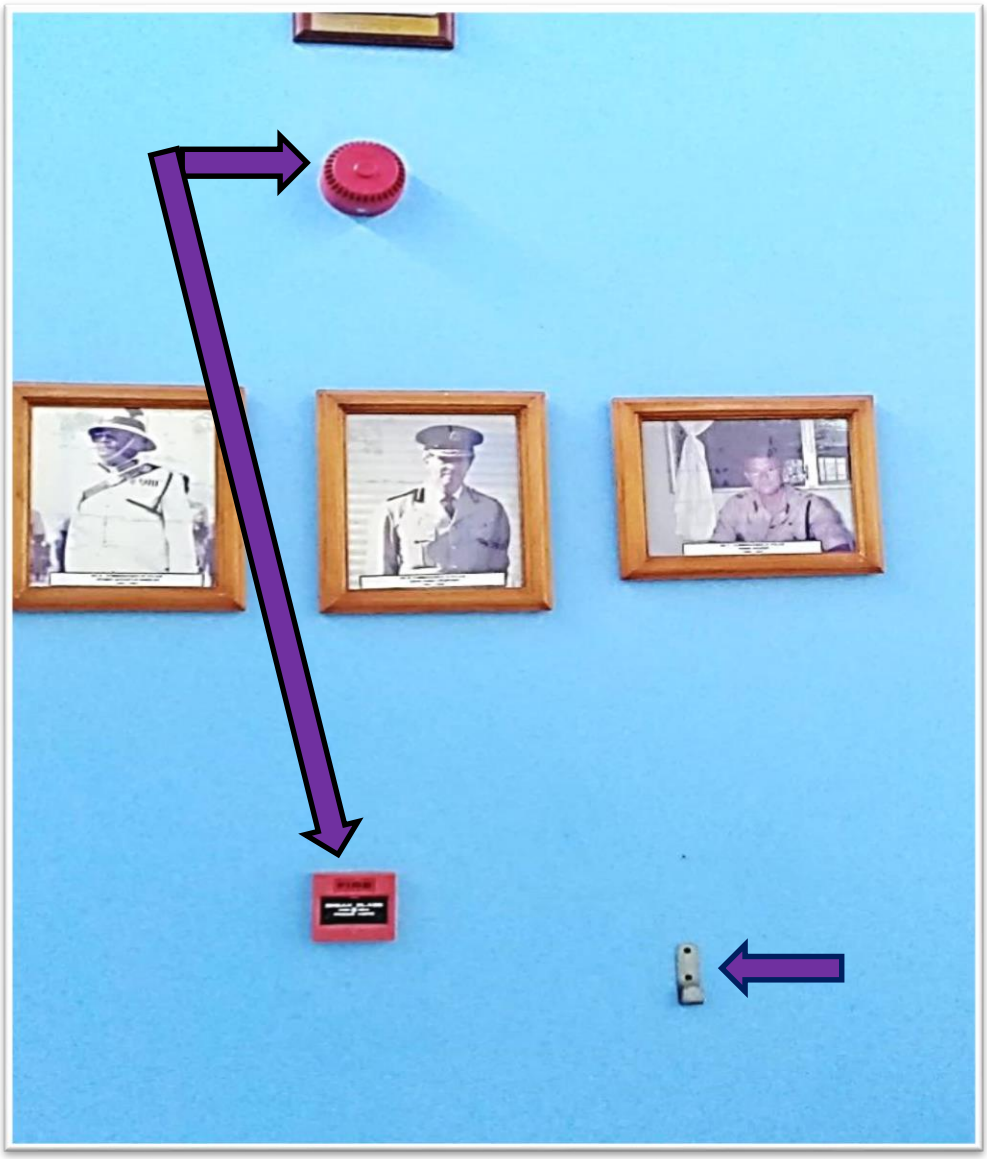
- Click here to install the New OTRCIS Client
- Click on the "Install" button
- Follow the on-screen instructions

Help

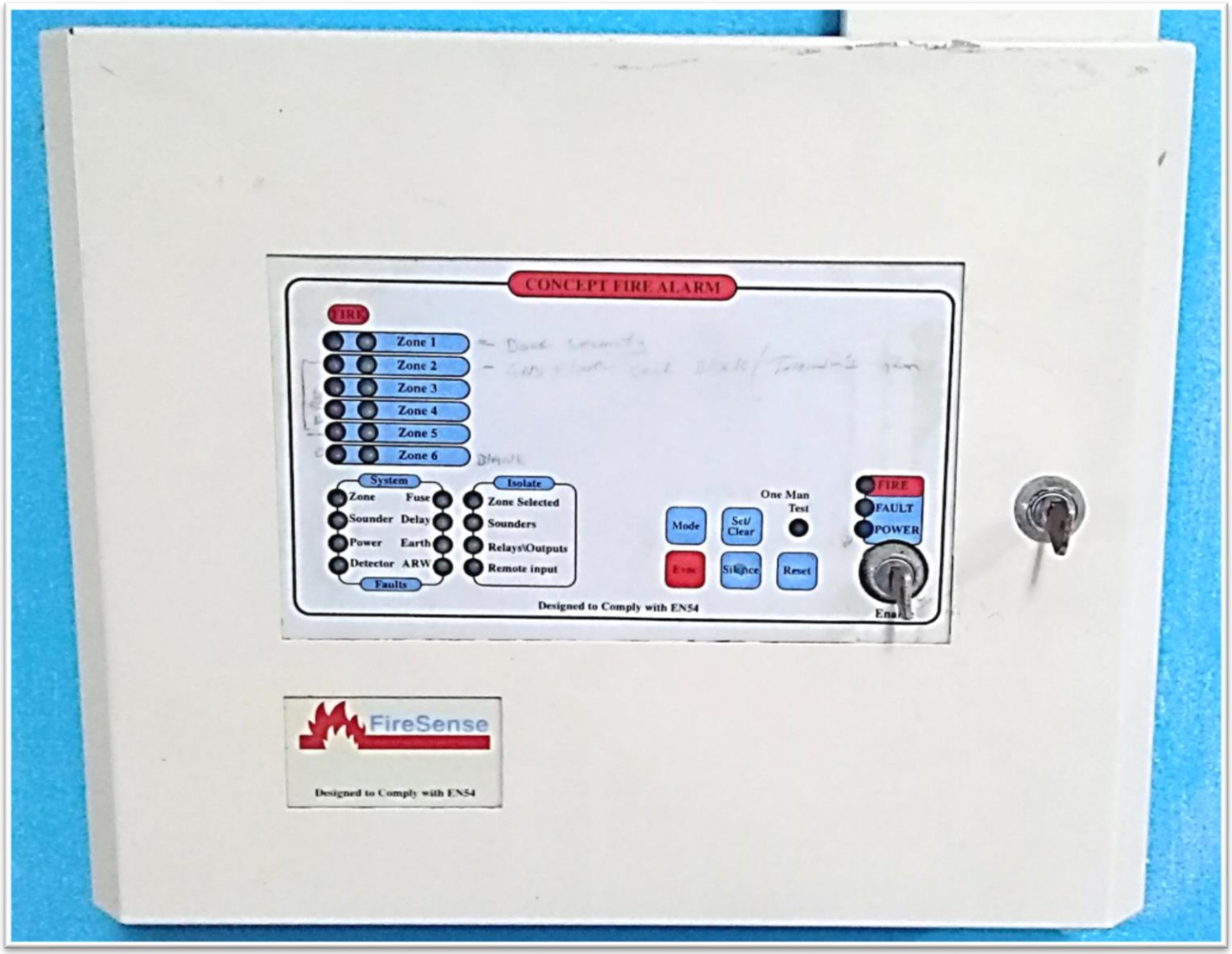
- Click here to download the New OTRCIS Hand out
- Right Click here and choose save target as.. to download the demonstration video



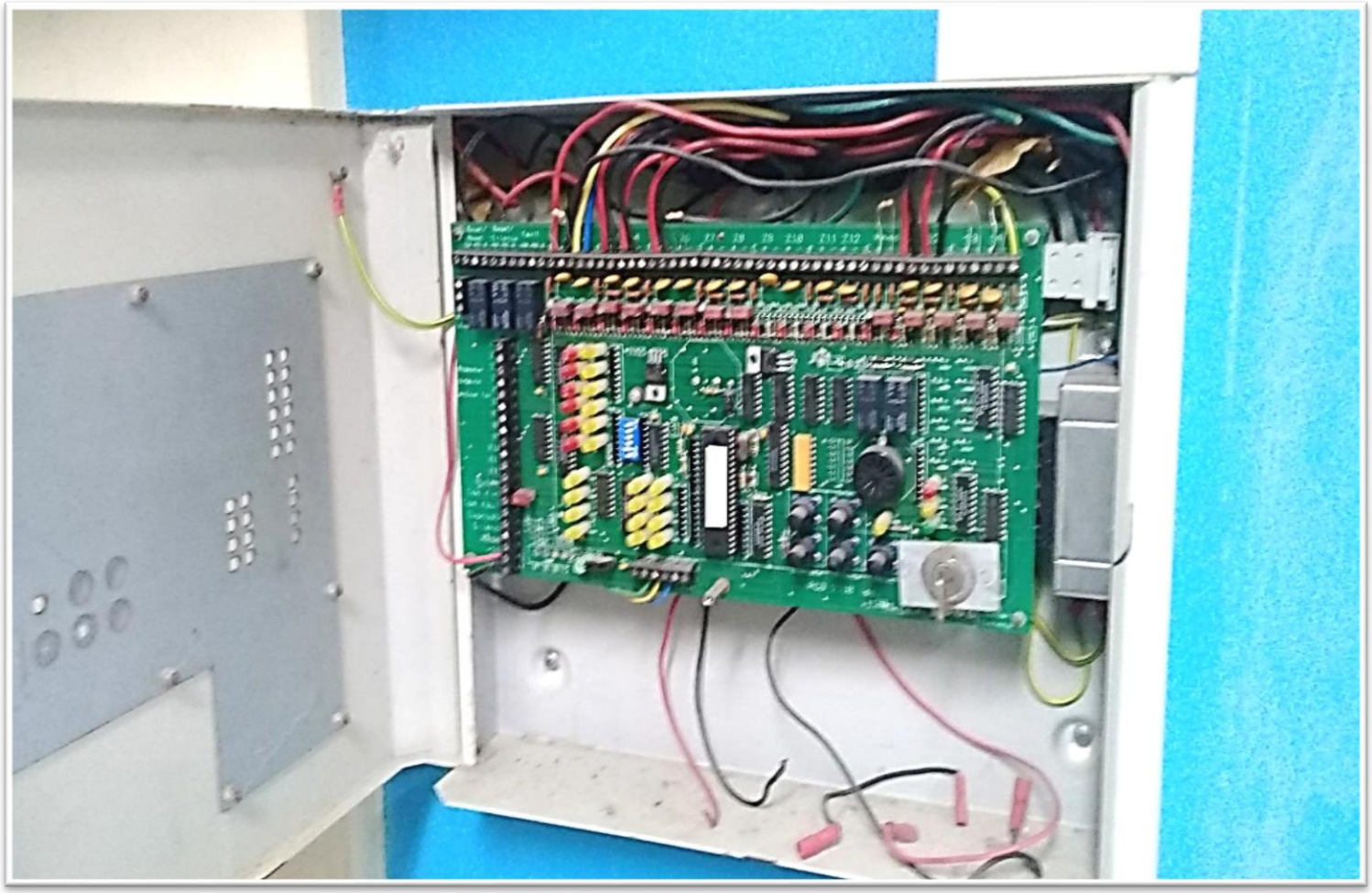
APPENDIX III - Non-Operational Fire Alarm System & Mounting Hook for Missing Fire Extinguisher



APPENDIX IV - Outer Cover of Defunct Emergency System Control Panel



APPENDIX V - Interior of Defunct Emergency System Control Panel



APPENDIX VI - Other RMPS Server Room Equipment

Appendix VII - Various Physical & Environmental Controls at Brades Police HQ