October 2017

AN INDEPENDENT AUDIT OF THE REGIONAL TRANSPORTATION MANAGEMENT CENTRE'S CYBERSECURITY CONTROLS

www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

CONTENTS

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1
P: 250.419.6100
F: 250.387.1230
www.bcauditor.com

The Honourable Darryl Plecas
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report, *An Independent Audit of the Regional Transportation Management Centre's Cybersecurity Controls.*

We conducted this audit under the authority of section 11 (8) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the CPA Handbook — Canadian Standard on Assurance Engagements (CSAE) 3001 and Value-for-money Auditing in the Public Sector PS 5400.

Carol Bellringer

Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
Date of Report: October 18, 2017

AUDITOR GENERAL'S COMMENTS

Carol Bellringer, FCPA, FCA
Auditor General

The Ministry of Transportation and Infrastructure's (ministry) Regional Transportation Management Centre (RTMC) serves as a major focal point for transportation management in the province. It's equipped with modern IT systems to manage traffic flow at major bridges and roadways in B.C., including lane controls on the Lions Gate Bridge, George Massey Tunnel and the Cassiar Tunnel.

In this audit, we focused on one aspect of traffic management. We looked to see if the RTMC had the foundational cybersecurity controls that are essential to any IT system. This includes controlling and monitoring access, keeping systems updated, and maintaining an inventory of systems and devices. We only looked at whether or not the cybersecurity controls were in place; we didn't assess their effectiveness.

Overall, we found that the ministry hasn't established appropriate cybersecurity controls to protect the RTMC's traffic management systems. At the time of our audit, there were significant gaps in the RTMC's cybersecurity controls.

For security reasons, we do not disclose findings that could put IT systems at risk. Instead, we provided the ministry with a detailed management letter that specifically outlines our findings and recommendations. We've recommended that the ministry work on these areas:

- knowing what hardware and software is in place
- establishing baseline settings for hardware and software
- performing vulnerability assessments and acting on the findings
- managing access to systems

AUDITOR GENERAL'S COMMENTS

Addressing these gaps will help ensure that the RTMC's traffic management systems are secure. The ministry is already taking steps to fill the gaps we identified. It's important that the ministry and the RTMC implement these recommendations because it's managing critical infrastructure and services for the people of B.C.

I'd like to thank the ministry for its co-operation during this audit.

Carol Bellringer

Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
October 2017

REPORT HIGHLIGHTS

RTMC **MANAGES TRAFFIC** at major bridges and roadways in B.C.

Audit focused on **FOUNDATIONAL CYBERSECURITY CONTROLS**

Audit identified **GAPS** in RTMC's **CYBERSECURITY CONTROLS**

Areas that need work include:

1. Knowing what hardware/software is in place
2. Establishing baseline settings for hardware and software
3. Performing vulnerability assessments and remediation
4. Managing access to systems

Ministry already **MAKING CHANGES** to fill the gaps

SUMMARY

In 2013, the Ministry of Transportation and Infrastructure (ministry) built the Regional Transportation Management Centre (RTMC) facility that now serves as a focal point for transportation management in the province. The RTMC is equipped with modern traffic control systems and provides 24/7, real-time monitoring of road and traffic conditions (of provincially managed highways) across B.C. Its goal is to keep traffic moving efficiently and safely.

Modern transportation systems are more advanced and more interconnected than ever before. This gives the RTMC remote access and control capabilities to manage traffic flow more efficiently. But, increased interconnectivity brings increased cybersecurity risk. These high levels of interconnectivity can result in a greater potential for significant disruption from a cybersecurity attack. For this reason, implementing appropriate cybersecurity controls is fundamental in keeping systems protected and maintaining a defensible security position.

Our audit examined whether the ministry has established appropriate cybersecurity controls to protect its traffic management systems operated out of the RTMC. We focused on the existence and design of controls, but we did not assess the operational effectiveness of the controls implemented.

Based on our audit, we concluded that the ministry has not established appropriate cybersecurity controls to protect its traffic management systems.

Security controls at the RTMC were not strong enough to protect its systems because the ministry has not properly:

- maintained a complete inventory of hardware and software
- managed system configurations
- validated systems through continuous vulnerability assessment and remediation
- controlled system administrative privileges

Without these foundational cybersecurity controls, the RTMC systems were at risk from cybersecurity threats.

In August 2017, we provided the ministry with a detailed technical report of our audit findings and recommendations, which we have summarized in this report. The ministry responded positively and stated that it has started addressing many of the deficiencies we identified. Ministry staff have also been working with the Office of the Chief Information Officer (OCIO) for remediation plans—both short-term and long-term—to address our findings and recommendations. We encourage the ministry to work collaboratively with the OCIO to address our recommendations.

OFFICE OF THE CHIEF INFORMATION OFFICER

The Office of the Chief Information Officer (OCIO) of the Ministry of Citizens' Services is responsible for providing technology, security and policy-related guidance and advice to ministries. Through its information security program, the OCIO provides support (such as information security awareness, vulnerability and risk management, and security operations) to ministries to ensure plans and processes are in place to appropriately manage information security risks within government programs.

SUMMARY OF RECOMMENDATIONS

WE RECOMMEND THAT THE MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE:

1 conduct risk assessments of the RTMC operational environment and ensure appropriate security controls are implemented.

2 maintain an inventory of all system components (hardware and software) authorized to access the RTMC networks and implement mechanisms to discover any unknown components on the network.

3 establish and maintain secure baseline configurations for all RTMC system components.

4 conduct ongoing vulnerability assessments and remediation for RTMC systems.

5 ensure that the use of system administrative accounts for RTMC systems is properly controlled.

RESPONSE FROM THE MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE

The Ministry of Transportation and Infrastructure would like to thank the Office of the Auditor General (OAG) for conducting the cybersecurity audit of its Regional Transportation Management Centre (RTMC) and for identifying opportunities for the ministry to improve the cybersecurity posture of its systems at the RTMC.

The ministry takes the security of its systems very seriously and accepts all five recommendations in the report.

The ministry has already taken the following prompt and appropriate actions to start addressing the recommendations. Working closely with the Office of the Chief lnformation Officer, the ministry has:

- updated its existing inventories of all hardware and software system components;
- conducted assessments to establish secure baseline configurations;
- performed vulnerability assessments and fixed any vulnerabilities found; and
- reviewed the management of systems' privileged accounts.

The ministry has also established teams to work diligently on addressing the remaining parts of each recommendation. These teams will:

- conduct a new risk assessment of the RTMC operational environment;
- maintain inventories on an ongoing basis and implement mechanisms to discover any unknown components on the network;
- establish and maintain secure baseline configurations for all RTMC system components;
- continue performing ongoing vulnerability assessments and fix any vulnerabilities found; and
- further improve the controlled use of system administrative accounts.

The public can be confident that safety will always be the ministry's top priority. The ministry has built its transportation systems in accordance with a fundamental engineering principle called fail-safe to prevent these systems from operating in an unsafe state. For example, as indicated in the report, "the ministry has a number of safety measures in place designed to prevent conflicting traffic signals on the same lane."

The RTMC has been operating safely and reliably since its opening in 2013. It is worth noting that, during this audit, the Office of the Auditor General did not assess the operational effectiveness of the existing controls.

RESPONSE FROM THE MINISTRY OF TRANSPORTATION AND INFRASTRUCTURE

All organizations operating in cyberspace face ever-changing and increasing security threats and are challenged to maintain a reasonable level of cybersecurity on an ongoing basis. When it comes to cybersecurity, there will always be more improvements that can be made.

The ministry appreciates the efforts of the OAG staff and their consideration of the ministry's input during this audit. We value the recommendations issued by the OAG, which will strengthen our ability to further protect the ministry's systems from potential cyberattacks.

BACKGROUND

The Ministry of Transportation and Infrastructure (ministry) provides transportation services and infrastructure for British Columbia. A major goal of the ministry is its commitment to provide a safe and reliable highway system, with strategies aimed to "move people and goods safely."

REGIONAL TRANSPORTATION MANAGEMENT CENTRE

In 2013, the ministry built the Regional Transportation Management Centre (RTMC) to help achieve its transportation goals. The facility now serves as a focal point for transportation management in the province (see Exhibit 1). The RTMC:

- monitors round-the-clock, real-time road and traffic conditions of provincially managed highways
- manages the lane operations of some bridges and tunnels in the Lower Mainland
- delivers traffic and road condition information to the travelling public
- supports traffic incident responses

The ministry manages traffic primarily through two specialized systems at the RTMC: an advanced traffic management system and a lane control system.

Advanced traffic management system

The advanced traffic management system at the RTMC integrates traffic data collected from field devices (e.g., cameras and sensors) (see Exhibit 2) as well as third-party information, such as weather data and law enforcement advisories.

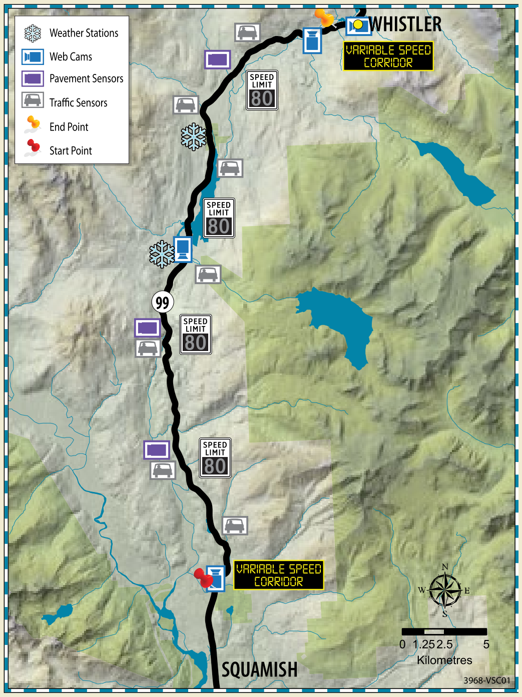
The system sends data to digital message signs and variable speed limit signs (see Exhibit 3) on roadways and traveller information websites (e.g., www.drivebc.ca). These public signs and websites help drivers optimize their travel plans with information on current traffic flow, estimated travel times, road and driving conditions, border crossing delays and traffic incident information.

Exhibit 1: RTMC facility

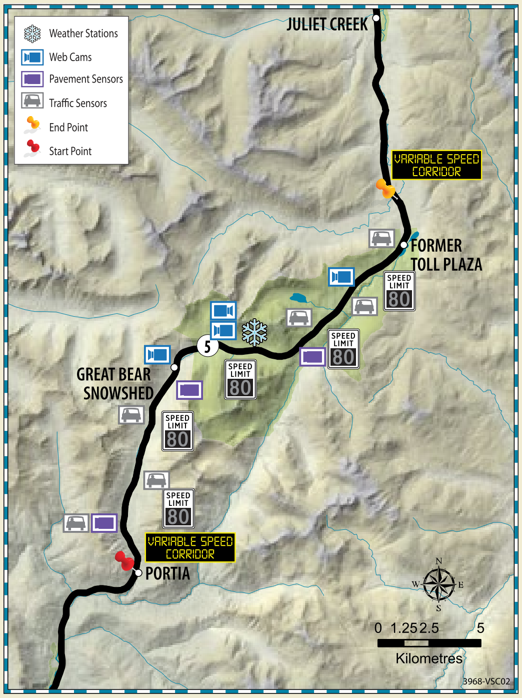
Source: www.tranbc.ca

BACKGROUND

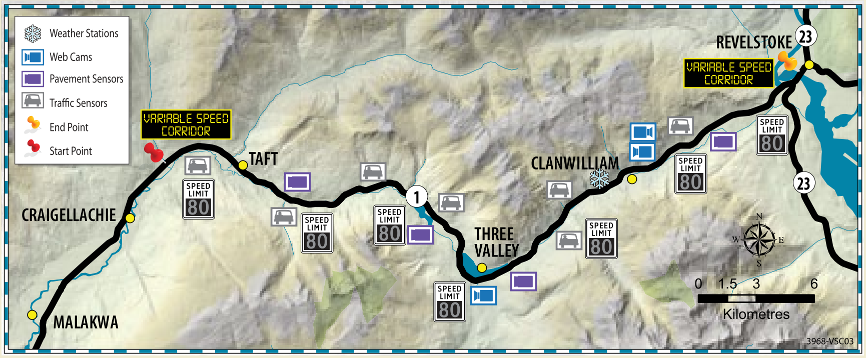
Exhibit 2: Field devices (e.g., web cameras, sensors and variable speed signs) along three BC highway corridors



Highway 99 – Sea-to-Sky between Squamish and Whistler



Highway 5 – Coquihalla between the Portia interchange and the former toll booth plaza



Highway 1 – west of Revelstoke between the Perry River Bridge and Highway 23 South interchange

Source: www2.gov.bc.ca

BACKGROUND

Exhibit 3: Variable speed limit sign

Source: news.gov.bc.ca

Lane control system

The ministry actively controls lane usage at three sites in the province, all of which are in the Lower Mainland. The sites are:

- Lions Gate Bridge (see Exhibit 4)
- George Massey Tunnel
- Cassiar Tunnel

Exhibit 4: Lions Gate Bridge with (reversible) centre lane operating in north-bound mode

Source: commons.wikipedia.org

The Lions Gate Bridge and George Massey Tunnel have *reversible* roadway lanes (the Cassiar Tunnel lanes are not reversible). A reversible lane allows RTMC operators to change traffic direction and improve traffic flow at tunnels and bridges, especially during peak periods. Lane change operators use a combination of traffic signals, control gates and monitoring cameras to reverse the direction of a traffic lane. The ministry has a number of safety measures in place designed to prevent conflicting traffic signals on the same lane.

Before the RTMC came into operation in 2013, operators were on-site to control the lane change operation. Since 2013, all lane control operations are handled centrally—made possible by the RTMC's advanced technologies. Now, by design, the ministry's lane controls are managed and controlled remotely by operators at the RTMC's control centre.

BACKGROUND

THE IMPORTANCE OF CYBERSECURITY CONTROLS

In the past, traffic control systems were separated from other networks and were physically secured and controlled by on-site operators. This meant there was less need for additional cybersecurity controls. But today's transportation systems, while more advanced, are more interconnected than ever before. As a result of the interconnectivity, there is more exposure to cybersecurity threats.

CYBERSECURITY THREATS

Cybersecurity threats are events or people that have the potential to act upon system vulnerabilities in a way that negatively impacts system confidentiality, integrity or availability. Human threats to systems may be outsiders (e.g., hackers connected via the internet) or insiders—both malicious (e.g., disgruntled staff) and well-intentioned (e.g., staff going around security policies for convenience).

A cybersecurity attack on traffic management systems could bring about large-scale traffic congestion or disrupt operations in a way that may cause safety issues. For this reason, it is vital for the ministry to protect its traffic management systems by implementing appropriate foundational cybersecurity controls and maintaining a defensible security position.

HOW FOUNDATIONAL CYBERSECURITY CONTROLS HELP REDUCE RISK

Inventory of hardware and software: By having a full picture of what should be running on its network, an organization can properly manage and control its systems' resources. This helps reduce the risk of unauthorized devices or applications being on the network without the organization's knowledge.

Configuration management: By having its systems properly configured in a known, trusted state, an organization can more readily discover unauthorized changes to hardware and software, as well as discover where authorized changes may be missing. This helps reduce the number of systems that are vulnerable to attack.

Vulnerability assessment and remediation: By having a process for ongoing detection of vulnerable systems and then fixing them as soon as possible, an organization can reduce the likelihood of systems remaining vulnerable.

Controlled use of administrative accounts: By limiting the use of administrative accounts and logging when they are used, an organization can attribute administrative actions to individual users. It can also monitor and analyze administrative activity to look for anomalies. This helps reduce the likelihood that unauthorized and inappropriate changes are made to the systems.

ABOUT THE AUDIT

AUDIT OBJECTIVE

THE OBJECTIVE OF our audit was to determine whether the Ministry of Transportation and Infrastructure has established appropriate cybersecurity controls to protect its traffic management systems.

AUDIT CONCLUSION

We concluded that the Ministry of Transportation and Infrastructure has not established appropriate cybersecurity controls to protect its traffic management systems.

BASIS FOR CONCLUSION

Based on our audit criteria (see Exhibit 5), we found that the ministry has not properly:

- maintained a complete inventory of hardware and software
- managed system configurations
- validated systems through continuous vulnerability assessment and remediation
- controlled system administrative privileges

AUDIT SCOPE AND APPROACH

Our audit focused on the existence and design of controls to protect the traffic management systems from cybersecurity threats. A weakness in the design or implementation of controls would be sufficient to determine if the ministry is appropriately managing related risks. We did not assess the operational effectiveness of the controls implemented.

The audit focused on the Ministry of Transportation and Infrastructure's (ministry) operations at the Regional Transportation Management Centre (RTMC). All information technology (IT) and system components housed in the RTMC and at the three sites with lane control were in scope for the audit. We did not audit whether the traffic management systems, including lane change, were operated or managed safely and reliably.

We carried out our work between April 2017 and May 2017. Our work involved:

- interviewing ministry and contract staff on IT security practices
- visiting the RTMC control centre and three sites with lane controls to observe and evaluate the control environment
- reviewing documentation from the ministry for supporting evidence of controls implemented
- verifying system settings and controls implemented

ABOUT THE AUDIT

AUDIT CRITERIA

We developed the audit objective and criteria based on the foundational controls set out in the cybersecurity best practices guide issued by the Center for Internet Security (CIS).

CIS CONTROLS

The Center for Internet Security (CIS) is a non-profit entity (based in the United States) that develops standards to safeguard organizations against cybersecurity threats. The CIS has issued 20 controls for organizations to improve their cybersecurity defense—controls referred to as *critical cybersecurity controls* or CIS controls.

We singled out the foundational CIS controls because they are known to eliminate the vast majority of an organization's cybersecurity vulnerabilities.

To determine whether the ministry has designed and implemented appropriate cybersecurity controls to protect its traffic management systems, we used the criteria in Exhibit 5.

AUDIT QUALITY ASSURANCE

We conducted this audit under the authority of section 11 (8) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the CPA Handbook—Canadian Standard on Assurance Engagements (CSAE) 3001 and Value-for-money Auditing in the Public Sector PS 5400. These standards require that we comply with ethical requirements, and conduct the audit to independently express a conclusion whether or not the subject matter complies in all significant respects to the applicable criteria.

Exhibit 5: Audit criteria

Audit criteria	What does this mean?
1. We expected the ministry to maintain and manage an inventory of authorized and unauthorized devices and software.	Know what hardware and software is connected to your systems and networks so you can secure it.
2. We expected the ministry to establish and manage the security configurations for hardware and software on all devices.	Secure systems and network devices with known, good settings and reinforce regularly.
3. We expected the ministry to continuously validate systems through vulnerability assessment and remediation.	Regularly identify system weaknesses and fix them.
4. We expected the ministry to control and manage the use of administrative privileges.	Limit and track system administrator account use, ensuring it is authorized and appropriate.

Source: Office of the Auditor General of British Columbia

ABOUT THE AUDIT

The Office applies the CPA Canadian Standard on Quality Control 1 (CSQC) and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. In this respect, we have complied with the independence and other requirements of the code of ethics applicable to the practice of public accounting issued by the Chartered Professional Accountants of BC, which are founded on the principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The report is dated October 18, 2017. This is the date the audit team completed obtaining the evidence used to base the findings and conclusions of the report, including the acceptance of a written representation from the Deputy Minister of the Ministry of Transportation and Infrastructure. The representation confirmed that we have been given the information we requested or that would substantially impact the findings and conclusions of the audit report.

KEY FINDINGS AND RECOMMENDATIONS

OVERALL, SECURITY CONTROLS AT THE RTMC NEED TO BE STRENGTHENED

WE LOOKED AT the Ministry of Transportation and Infrastructure's (ministry) implementation of cybersecurity controls at the RTMC. We found that security controls at the RTMC were not strong enough to properly protect its systems from cybersecurity threats. This puts systems at risk of internal and external attack.

The audit highlighted a need for the ministry to strengthen its effort in managing cybersecurity risks and controls at the RTMC.

RECOMMENDATION 1: *We recommend that that the Ministry of Transportation and Infrastructure conduct risk assessments of the RTMC operational environment and ensure appropriate security controls are implemented.*

A COMPLETE INVENTORY OF HARDWARE AND SOFTWARE WAS NOT MAINTAINED

Knowing what hardware and software are running on the network is fundamental to managing cybersecurity risks. Inventorying all hardware (devices) and software (applications) helps organizations understand their resources and establish a baseline for managing system changes, security patches and recovery.

We expected to find that the ministry maintained a complete inventory of RTMC hardware and software so it could track and control the devices and applications that were authorized to run on the network. We also expected to find that the ministry monitored what was connected and running on its network to detect any unauthorized devices or software.

We found that:

- The ministry did not update and maintain a complete inventory.
- The ministry did not have a way of detecting and reporting what was running on its network.

RECOMMENDATION 2: *We recommend that the Ministry of Transportation and Infrastructure maintain an inventory of all system components (hardware and software) authorized to access the RTMC networks and implement mechanisms to discover any unknown components on the network.*

KEY FINDINGS AND RECOMMENDATIONS

SYSTEM CONFIGURATION MANAGEMENT WAS NOT IN PLACE

Systems in their default state (factory configured settings) are likely vulnerable to a wide range of threats. Organizations address this by developing baseline configuration standards. In doing so, organizations can quickly and reliably bring systems back to their known, secure states after component failure, misconfiguration or when a compromise is suspected.

CONFIGURATION STANDARDS

Configuration standards are established baselines applicable to all hardware and software components that impact an organization's network operations and security. The purpose is to strengthen the security of the organization's systems. These standards vary between organizations and must be aligned to the organization's operational and security policy and risks. Examples of good configuration standard practices include:

- enforcing strong password requirements to prevent unauthorized system access
- removing unnecessary software to limit exposure to vulnerabilities
- applying software updates (security patches) to fix known vulnerabilities
- installing anti-virus software protection on system servers

We expected to find that the ministry had established baseline configuration standards for its systems. We also expected that the ministry had configuration management processes in place to actively manage and update configuration standards, and identify changes on critical systems for indications of unwanted change.

We found that:

- The ministry had not established baseline configuration standards for all its systems.
- A configuration management process was not in place to continually manage and update the baseline configuration settings of critical systems, and monitor them for configuration changes.

RECOMMENDATION 3: *We recommend that the Ministry of Transportation and Infrastructure establish and maintain secure baseline configurations for all RTMC system components.*

KEY FINDINGS AND RECOMMENDATIONS

NO ONGOING PROCESS FOR VULNERABILITY ASSESSMENT AND REMEDIATION

Vulnerability assessments are an important mechanism for organizations to identify potential security exposures and to assess and remediate them. Early detection allows organizations to address the deficiencies before attackers can exploit them. Performing regular vulnerability assessments will reduce the likelihood of a vulnerability remaining undiscovered and improve the organization's security position.

VULNERABILITY ASSESSMENT

Vulnerabilities are weaknesses in a computer, network or communications infrastructure. An example of a vulnerability is the presence of a computer with an outdated operating system (it is often easy to break into such systems until they are updated). A vulnerability assessment involves the identification, quantification and prioritization of vulnerabilities.

We expected to find that the ministry had established processes for continuous vulnerability assessment and proactively addressed discovered flaws.

We found that:

- The ministry performed a vulnerability scan when the RTMC was first established.
- There was no ongoing process for vulnerability assessment and remediation.

RECOMMENDATION 4: *We recommend that the Ministry of Transportation and Infrastructure conduct ongoing vulnerability assessments and remediation for RTMC systems.*

KEY FINDINGS AND RECOMMENDATIONS

SYSTEM ADMINISTRATIVE PRIVILEGES WERE NOT PROPERLY CONTROLLED

System administrative accounts are powerful accounts that have an elevated level of access, beyond the access given to regular accounts, so that administrators can manage systems and provide system support. Ineffective management of these accounts may contribute to system failures and security breaches.

SYSTEM ADMINISTRATORS

System administrators are responsible for maintenance, configuration and reliable operation of computer systems. Their functions include: installing software, resetting passwords, creating or disabling accounts and updating security configurations.

We expected to find that the system administrative accounts were properly controlled with the correct people being assigned to the accounts and with account activity limited and tracked to ensure it was authorized and appropriate.

We found that:

- The ministry lacked proper control over the system administrative accounts.

RECOMMENDATION 5: *We recommend that the Ministry of Transportation and Infrastructure ensure that the use of system administrative accounts for RTMC systems is properly controlled.*

AUDIT TEAM

Morris Sydor
Assistant Auditor General

Ada Chiang
Director, IT Audit

John Bullock
Senior IT Audit Specialist

Greg Morhart
IT Auditor

OFFICE OF THE
Auditor General
of British Columbia

Location

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

Office Hours

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll free through Enquiry BC at: 1-800-663-7867
In Vancouver dial: 604-660-2421

Fax: 250-387-1230

Email: bcauditor@bcauditor.com

Website: www.bcauditor.com

This report and others are available at our website, which also contains further information about the Office.

Reproducing

OFFICE OF THE

Auditor General

of British Columbia