Ministry of Transportation and Infrastructure

An Independent Audit of The Regional Transportation Management Centre's Cybersecurity Controls Released October 2017
http://www.bcauditor.com/pubs

PAC Meeting Plan[1]	**[16/01/18]**	**Prepared by: Caner Budakoglu, Ministry of Transportation and Infrastructure**	**Reviewed by: Kevin Richter ADM Associate Deputy Minister's Office, Nancy Bain ADM Finance and Administrative Services**
1st APPA Update	**[26/02/19]**	**Prepared by: Carlos Caraveo, Ministry of Transportation and Infrastructure**	**Reviewed by: Kevin Richter ADM Associate Deputy Minister's Office, Nancy Bain ADM Finance and Administrative Services**
2nd APPA Update	**[26/02/20]**	**Prepared by: Debbie Fritz, Ministry of Transportation and Infrastructure**	**Reviewed by: Kevin Richter ADM Associate Deputy Minister's Office, Nancy Bain ADM Finance and Administrative Services**
3rd APPA Update	**[24/02/21]**	**Prepared by: Carlos Caraveo, Ministry of Transportation and Infrastructure**	**Reviewed by: Kevin Richter ADM Associate Deputy Minister's Office, Nancy Bain ADM Finance and Administrative Services**

[1] The audited organization will be required to present their initial action plan at this meeting (i.e. First three columns completed for each OAG recommendation included in the audit report)
Please provide your email response to:
Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
1 *Yes*	We recommend that the Ministry of Transportation and Infrastructure conduct risk assessments of the RTMC operational environment and ensure appropriate security controls are implemented.	The Ministry of Transportation and Infrastructure will perform a subsequent risk assessment for the RTMC operational environment once all actions are completed. **Target Date**: 31/12/2019	**Progress Assessment:** Fully or substantially implemented **Actions Taken to meet the Recommendation:** The Ministry of Transportation and Infrastructure has conducted a risk assessment of the RTMC operational environment based on the Auditor General's findings. In addition, a physical security assessment was also performed with improvements made to both the Local Operating Centres and the RTMC data centre. **Additional Proactive Activities:** • Regular follow-up assessments performed with inventory maintained • Additional assessments are performed as each of the RTMC systems are replatformed into the remediated environment. • A Core Network upgrade is underway that will include industrial control system passive vulnerability scanning – 31/05/2021 (This activity was delayed do to COVID. This impacted procuring of network devices and having resourcing onsite for installation and troubleshooting) • Physical upgrades continue at each of the Local Operating Centres (Physical security has been upgraded, true server rooms with additional security and monitoring have been implemented, power has been upgraded) • Review and update Risk Assessment/Register on annual basis at minimum • As part of the Core Network Upgrade and the choice to work with Telus and the Office of the Chief Information Officer (OCIO), MOTI has implemented network management tools – all used to monitor and report on both the Core Network and the Field Network.

[2] For each recommendation, the audited organization should state whether or not they have accepted the recommendation and plan to implement it fully by typing either "Yes" or "No" under the number of the recommendation.
[3] Target date is the date that audited organization expects to have "fully or substantially implemented" the recommendation. If several actions are planned to implement one recommendation, indicate target dates for each if they are different.
[4]The Select Standing Committee on Public Accounts (PAC) will request that the audited organization provide a yearly update (i.e completed "Assessment of Progress and Actions Taken" column) until all recommendations are fully implemented or otherwise addressed to the satisfaction of the PAC. This is for the APPA update.
[5] This action plan and the subsequent updates have not been audited by the OAG. However, at a future date that Office may undertake work to determine whether the entity has implemented the recommendations. The results of that work will be reported in a separate report prepared by the OAG.

Please provide your email response to:
Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
2. *Yes*	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.	The Ministry of Transportation and Infrastructure is maintaining inventories on an ongoing basis and is investigating systems to help. **Target Date:** 3/10/2018	**Progress Assessment:** Fully or substantially implemented **Actions Taken to meet the Recommendation:** The Ministry of Transportation and Infrastructure has completed an inventory of all system components authorized to access the RTMC networks. Also implemented is an ongoing discovery process for any system components that are unknown to the network and the remediation of those components (removal or authorized access). Through this process an overall inventory is managed and kept up to date. **Additional Proactive Activities:** • A vulnerability scanning solution has been purchased and will be implemented once the Core Network Upgrade is complete. This will allow for automated discovery of devices on the network and allow for the process of managing authentication – Implementation is underway and will be complete 31/05/2021

Please provide your email response to:
Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
3. *Yes*	We recommend that the Ministry of Transportation and Infrastructure establish and maintain secure baseline configurations for all RTMC system components.	The Ministry of Transportation and Infrastructure is establishing and will maintain secure baseline configurations for all RTMC system components **Target Date**: 31/12/2019	**Progress Assessment:** Fully or substantially implemented **Actions Taken to meet the Recommendation:** The Ministry of Transportation and Infrastructure in working with the OCIO and associated support teams has created and are maintaining secure baseline configurations for all workstations, servers and network system components that are a part of the overall RTMC system. **Additional Proactive Activities:** While the Ministry satisfied the OAGs requirements by Dec 2019 the Ministry is continuing to improve by: • As each system and component is remediated and transitioned it is taken through a standard set of validation and remediation tasks to ensure it meets the standards set above. System and component transition will continue until December 31, 2021. • In addition to configuration, extended security measures have been put in place through the development of an OCIO standard micro-data centre at the RTMC. First of its kind, the RTMC micro-data centre provides the same level of security, configuration, and management as the Kamloops data centre but on a smaller scale. Along with this infrastructure and configuration all components will be brought into OCIO managed environments wherever possible. Any components that must be maintained in parallel for a transition period are following OCIO standards for configuration, security, and management processes. • The RTMC Micro-Data centre is part of the regular operational processes for standard patching and upgrades.

Please provide your email response to:
Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
4. *Yes*	We recommend that the Ministry of Transportation and Infrastructure conduct ongoing vulnerability assessments and remediation for RTMC systems.	The Ministry of Transportation and Infrastructure will perform monthly vulnerability assessments and fix any new vulnerabilities found. **Target Date:** 30/06/2018	**Progress Assessment:** Fully or substantially implemented **Actions Taken to meet the Recommendation:** The Ministry of Transportation and Infrastructure along with the assistance of the OCIO Security Team have conducted a full vulnerability assessment of the RTMC and its systems. To assist with ongoing and regularly schedule vulnerability assessments a joint Risk Register has been created and maintained to track and rate vulnerabilities. **Additional Proactive Activities:** • The Ministry of Transportation and Infrastructure along with standard support processes from the OCIO have implemented regular ongoing monthly External Vulnerability Scans as well as ongoing quarterly Internal Vulnerability scans. As each system is replatformed vulnerability scans are executed as part of the standard replatforming methodology. • A vulnerability scanning solution has been purchased and will be implemented once the Core Network Upgrade is complete. This will allow for automated discovery of devices on the network and allow for the process of managing authentication – Implementation is underway and will be complete 31/05/2021

Rec. # Accepted? Yes / No[2]	OAG Recommendations	Actions Planned & Target Date(s)[3]	Assessment of Progress to date[4] and Actions Taken[5] (APPA update)
5. *Yes*	We recommend that the Ministry of Transportation and Infrastructure ensure that the use of system administrative accounts for RTMC systems is properly controlled.	The Ministry of Transportation and Infrastructure is continuing to make further improvements on the controlled use of system administrative accounts. **Target Date:** 31/12/2019	**Progress Assessment:** Fully or substantially implemented **Actions Taken to meet the Recommendation:** The Ministry of Transportation and Infrastructure along with members of the OCIO support teams for workstations, servers and networks have completed a review of current administrative account configurations, procedures, users, and documentation for all items included in workstations, servers, and networks. **Additional Proactive Activities:** • The Ministry of Transportation and Infrastructure along with its OCIO partners have put in place ongoing administrative activities. These ongoing activities allow for the assigning, controlling, and monitoring of administrative access. As the RTMC managed network grows through the ongoing remediation of systems these tools will continue to expand and improve with additions of automated technologies, administrative dashboards and console technology for the automated management and tracking of access, and to include in their inventory each remediated system and its components. • OCIO IDIR Administrative accounts are utilized for both server management, line of business software management and network devices. • Requests are made to the OCIO to create the accounts with core policy in place for password management and reset. • For each person that requires administrative access whether it be server related, line of business software related, or network related, the access request must follow a standard process for approval and tracking. • The same applies for each resource as they may leave the project or Ministry.

Please provide your email response to:
Email: Comptroller General's Office of the Government of British Columbia Comptroller.General@gov.bc.ca
Cc email to: the Office of the Auditor General of British Columbia actionplans@bcauditor.com