March 2017

POLICE RECORDS INFORMATION MANAGEMENT ENVIRONMENT: PRIME-BC SYSTEM – A SECURITY AUDIT

www.bcauditor.com

CONTENTS

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

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

Dear Madame Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report *Police Records Information Management Environment: Prime-BC System – A Security Audit.*

We conducted this audit under the authority of sections 13(1)(b) and 13(3) 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 - Assurance and Value-for-Money Auditing in the Public Sector, Section PS 5400.

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

AUDITOR GENERAL'S COMMENTS

Carol Bellringer, FCPA, FCA
Auditor General

In 2013, we audited PRIME-BC—a province-wide IT system for the police. Because we were dealing with sensitive police data and our findings could have further exposed the system, we did not publicly release a report. We do not disclose findings that could put IT systems at risk.

In 2016, we completed a second audit of PRIME-BC. Not a progress or follow-up audit as we often do, but rather a second full audit. Again, some of our results show security weaknesses which could potentially expose the system if reported, hence this short report.

That said, the *Auditor General Act* requires that we publicly report on our audits. PRIMECorp (the organization that manages PRIME-BC) has made progress on implementing our recommendations, which has reduced the risk of exposure. There was a risk, at the time of our 2013 audit, that the system could be breached. There are still vulnerabilities but PRIME-BC has good controls to protect against external attacks. PRIMECorp is still working to strengthen internal security.

We made one recommendation in this report. PRIME-BC should be protected with multiple layers of security, so it's very important that the PRIMECorp board of directors ensure management implements the recommendations as provided in our detailed management report. We will not publicize our detailed recommendations, as regardless of the level of risk, it is not our intention to provide a road map which could compromise the system.

I would like to thank PRIMECorp for their cooperation with this audit, and our 2013 audit.

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

REPORT HIGHLIGHTS

PRIME-BC contains **SIGNIFICANT** and **SENSITIVE** INFORMATION

PRIME-BC is essential to **POLICE SERVICES**

2013
no public report due to **SENSITIVE FINDINGS**

2016
PRIMECorp made **IMPROVEMENTS** but needs to do

MORE

Controls in place to protect against **EXTERNAL ATTACKS**

STRONGER **CONTROLS** needed to **PREVENT** internal **THREATS**

RECOMMENDATION

WE RECOMMEND THAT:

1 the board of directors ensure PRIMECorp implements the recommendations in our detailed management report.

RESPONSE FROM PRIMECORP

Securing and protecting the information that British Columbia's police agencies enter into the Police Records Information Management Environment (PRIME-BC) is PRIMECorp's top priority.

With that in mind, we thank the Office of the Auditor General (OAG) for its comprehensive analysis of PRIME-BC's information technology security controls and the valuable recommendations provided to us. By accepting all recommendations and working diligently to prioritize and implement them, we were able to enhance existing safeguards and achieve the significant changes noted in the OAG's 2016 audit report.

The OAG advised PRIMECorp in 2013 that PRIME-BC was protected from external cyberattacks and we are pleased that the OAG has again concluded that there are adequate perimeter controls protecting PRIME-BC from external attacks launched from the Internet. We understand that there are further enhancements required in order to detect and prevent potential cyberattacks launched from within the internal network and we appreciate the recommendations we received from its experts in this area. We will continue to work to maintain vigilance with regard to the prevention, early detection and swift mitigation of any threat, internal or external, that may impact PRIME-BC.

The PRIMECorp board of directors accepts the recommendation of the OAG, and will, on a quarterly basis, monitor the progress of the implementation of the remaining recommendations, which are anticipated to be complete by the end of 2017.

One point in the report requires clarification. PRIMECorp is accountable to a board of directors and operates under a governance structure with accountability to a number of stakeholders. We would be pleased to provide further information and documentation to the Office of the Auditor General explaining the governance structure in detail.

As the custodians of the police information entered into the PRIME-BC shared system, PRIMECorp understands the special role it plays in maintaining the security of that information for both public safety and officer safety. The work completed by the Auditor General will help PRIMECorp and all British Columbia police agencies face the increasing, and always evolving, security threats that face all organizations and governments in today's cyber world.

BACKGROUND

Police Records Information Management Environment (PRIME-BC) is the computerized system that provides police with immediate, real-time access to critical information about criminals and crimes. The system records occurrences from the first point of contact with police, including 911 calls, through to the completion of investigations and reports.

PRIME-BC is essential to the success of police operations and key to effective policing in B.C. It is linked to a dispatch system and mobile workstations in police cars, which allows continuous communication at all times. From their police cars, officers can access records and respond to emergency calls. And from call centres, dispatchers use integrated maps to locate and dispatch police cars.

Having a common system for all municipal police agencies and Royal Canadian Mounted Police (RCMP) detachments across B.C. gives police the ability to exchange information quickly and efficiently. PRIME-BC is also linked to other police systems across Canada. This means immediate access to information outside of B.C.

Approximately 13,000 users from 13 municipal police agencies and about 135 RCMP detachments are connected to PRIME-BC. These users include police officers and investigators, 911 operators, dispatchers and other police agency support personnel.

Since 2003, Police Records Information Management Environment Incorporated (PRIMECorp) has managed PRIME-BC. PRIMECorp is accountable to the Ministry of Public Safety and Solicitor General, and exists solely to manage PRIME-BC and support the delivery of B.C. police services. PRIMECorp is governed by a board of directors with representation from municipal police, the RCMP, Emergency Communications for B.C, municipalities and the Ministry of Public Safety and Solicitor General.

WHAT WE DID

In 2013, we examined the security controls in the PRIME-BC system but decided not to publicly release our audit because of the sensitivity of the findings. We issued an internal management report with detailed recommendations to PRIMECorp and monitored their progress in addressing the recommendations.

The focus of our 2016 audit was to assess if controls were in place to protect PRIME-BC from threats, including unauthorized access. To do this, we contracted with experts who assisted in analyzing the existence and adequacy of security controls, given the potential impacts of a system breach.

We developed our audit objective and criteria based on the international standards issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC): *ISO/IEC 27002 on Information Technology – Security Techniques – Code of Practice for Information Security Controls.*

http://www.iso27001security.com/html/27002.html

We conducted our audit in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the CPA Canada Handbook – Assurance and Value-for-Money Auditing in the Public Sector, Section PS 5400, and under the authority of sections 13(1)(b) and 13(3) of the *Auditor General Act*.

We conducted our initial audit from March 2013 to July 2013, and we conducted our re-audit from January 2016 to June 2016.

WHAT WE FOUND

We found that PRIMECorp has made significant changes to improve security since our 2013 audit, but controls are not strong enough to properly protect the system from all cyber threats. The consequences of not keeping up with best practices in security could compromise public and police safety. PRIME-BC has highly sensitive and confidential data and should be protected with multiple layers of security.

There are adequate perimeter controls protecting PRIME-BC from external attacks initiated from the Internet; however, the security controls may not adequately detect or prevent attacks initiated from inside the PRIME-BC network. We found areas for improvement and have made additional recommendations in a detailed management report. This includes recommendations that will put PRIMECorp in a better position to restore system operations from physical damage (e.g., earthquake, fire) or cyber attacks.

RECOMMENDATION 1: *We recommend that the board of directors ensure PRIMECorp implements the recommendations in our detailed management report.*

BOARD OF DIRECTORS

A ten-member board of directors oversees PRIMECorp, and is chaired by the Director of Police Services, from the Ministry of Public Safety and Solicitor General. The board has senior police officials and representatives from both municipal and provincial government and is responsible for the PRIMECorp's strategic direction, and financial and operational results.

AUDIT TEAM

Cornell Dover,
Assistant Auditor General

Pam Hamilton,
IT Audit Director

Ada Chiang,
IT Audit Director

Adel Elassal,
IT Consultant

Jamie Giroux,
IT Consultant

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