Chapter 27
SaskBuilds and Procurement—Web Application Security Requirements

1.0 Main Points

The Ministry of SaskBuilds and Procurement is responsible for the security requirements for the development and operation of web applications owned by various provincial government ministries (e.g., Justice and Attorney General, Finance).[1,2] The Ministry develops and hosts web applications in a data centre for ministries. Web applications may allow attackers to access and corrupt confidential government information, or interrupt government services, if not appropriately secured.

By January 2021, the Ministry made improvements to better support the development and operation of secure ministry web applications. It set clear guidance for checking new web applications are secure before they are put to use. Furthermore, it systematically looks for vulnerabilities in web applications and takes a risk-informed approach to address identified vulnerabilities.

Addressing high-risk vulnerabilities in ministry web applications helps minimize the risk of a breach of confidential government information in the web applications, and sensitive data being lost or inappropriately accessed.

2.0 Introduction

As of January 31, 2021, the Ministry of SaskBuilds and Procurement had identified 24 web applications as critical and 292 web applications as non-critical. Web applications classified as critical are those that are crucial for the everyday operations of government ministries (e.g., criminal justice information system).

Comprehensive security requirements support an organized and consistent approach to implementing and maintaining security across ministry web applications to help minimize the risk of a breach of government information.

2.1 Focus of Follow-Up Audit

This chapter describes our second follow-up audit of management's actions on the two outstanding recommendations we first made in 2016 about the Ministry of SaskBuilds and Procurement's security requirements for the development and operation of web applications.

Our *2016 Report – Volume 1*, Chapter 6, concluded that while the Ministry had an overall security policy framework consistent with best practices, for the twelve-month period ending

[1] Web applications are computer programs that are built into websites, and help websites work. For example, web applications are used when filling out a form, creating an account, using an online shopping cart, or using the search capability on a website.
[2] The Ministry of Central Services became the Ministry of SaskBuilds and Procurement in November 2020.

December 31, 2015, it did not have sufficiently comprehensive procedures and guidance to support the development and operation of secure government ministry web applications. We made four recommendations. By June 2018, the Ministry had addressed two of the four recommendations.[3]

To conduct this audit engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook—Assurance* (CSAE 3001). To evaluate the Ministry's progress toward meeting our recommendations, we used the relevant criteria from the original audit. Ministry management agreed with the criteria in the original audit.

We reviewed and assessed the Ministry's policies and procedures, scans of web applications, tracking of vulnerabilities identified, and measures taken to address vulnerabilities.

3.0 STATUS OF RECOMMENDATIONS

This section sets out each recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation at January 31, 2021, and Ministry's actions up to that date.

3.1 Guidance and Work to Address Web Application Vulnerabilities Appropriate

We recommended the Ministry of SaskBuilds and Procurement (formerly Ministry of Central Services) develop and maintain comprehensive procedures and guidelines to support the development and operation of secure web applications. (*2016 Report – Volume 1,* p. 51, Recommendation 2; Public Accounts Committee agreement January 11, 2017)

Status—Implemented

We recommended the Ministry of SaskBuilds and Procurement (formerly Ministry of Central Services) work with the ministries to address identified higher-risk web application vulnerabilities. (*2016 Report – Volume 1,* p. 54, Recommendation 4; Public Accounts Committee agreement January 11, 2017)

Status—Implemented

The Ministry of SaskBuilds and Procurement has appropriate guidance to support the development of secure web applications and identify vulnerabilities in existing applications. Even though the Ministry has appropriate processes to identify and prioritize vulnerabilities for mitigation, ministry web applications continue to have vulnerabilities.

In November 2018, the Ministry developed an Application Security Coding Guideline to outline principles for secure development of new web applications. The principles require web application developers to avoid common security issues identified by the security

[3] *2018 Report - Volume 2*, Chapter 28, pp.211-214.

industry. The Ministry also developed a Web Application Security Policy in January 2019 requiring security assessments of new web applications before putting them into use.

For two new web applications we examined, we found, consistent with its policy, the Ministry completed the security assessment prior to putting the new web application into use.

The Ministry developed a Vulnerability Management Process in May 2016, and last updated the policy in September 2019. These outline the frequency in which it expects to scan web applications for vulnerabilities. Effective November 2020, it expects critical web applications to be scanned quarterly and non-critical web applications annually.

We found the Ministry's Vulnerability Management Process, Web Application Security Policy and Application Security Coding Guidelines align with good practice.

Web application vulnerability scans identify various levels of vulnerabilities (e.g., critical, high, medium, and low). The Ministry addresses higher-risk critical vulnerabilities quicker than lower ranked ones (see **Figure 1**). It tracks vulnerabilities along with its status of implementing the planned mitigation (e.g., deploy encryption, restrict access, upgrade a system) in its IT service management system.

Figure 1—Vulnerabilities Levels and Associated Mitigation Timeframes

Vulnerability Level	Mitigation Timeline
Critical	24–48 hours
High	1 month
Medium	6 months
Low	Keep under periodic review

Source: Ministry of SaskBuilds and Procurement's Vulnerability Management Process.

For five existing web applications scanned by the Ministry in 2020, we tested:

- Two had mitigations ongoing at the time of our test, but were within the six-month target timeline for mitigation of medium vulnerabilities; the Ministry expected to complete the mitigation by March 31, 2021
- One was partially mitigated awaiting a server upgrade
- Two did not require mitigation

We found the Ministry appropriately entered vulnerabilities identified through the web-application scans into its IT service management system, and was mitigating the higher-risk vulnerabilities first.

Given the ever-changing nature of IT, some ministry web applications will always contain certain vulnerabilities. Having a systematic process to identify the existence of vulnerabilities, and prioritize the mitigation of those identified as critical is essential. Taking a risk-informed approach by compiling, prioritizing, and addressing higher-risk vulnerabilities reduces the risk that ministry web applications can be compromised, and sensitive data lost or inappropriately accessed.

(this page intentionally left blank)