Chapter 28
Central Services—Web Application Security Requirements

1.0 Main Points

Web applications may allow attackers to access and corrupt confidential government information or interrupt government services if not appropriately secured.

By June 2018, the Ministry of Central Services had made some improvements to better support the development and operation of secure government ministry web applications. It had addressed two of four recommendations we made in our 2016 audit related to web application security requirements. It was making progress on the other two recommendations.

Central Services was tracking key information about ministry web applications and had begun to assess web applications for security vulnerabilities. While it had started updating security-focused web application procedures and guidelines, further guidance was needed for prioritizing work to address identified high-risk vulnerabilities on a timely basis.

Addressing high-risk vulnerabilities in web applications helps minimize the risk of a breach of government information in the web applications, as well as in other applications and data that Central Services hosts in the data centre.

2.0 Introduction

The Ministry of Central Services is responsible for the security requirements for the development and operation of government ministry web applications.[1] 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. Sufficiently comprehensive procedures and guidance would include working with the ministries to promptly identify and address identified web application vulnerabilities classified as higher risk.

In our *2016 Report – Volume 1*, Chapter 6, we concluded that, while the Ministry of Central Services had an overall security policy framework consistent with best practices, 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.

This chapter is our first follow-up on the status of implementation of those recommendations.

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

[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.

original audit. We reviewed Central Services' web application security procedures and guidance, web application inventory systems, results of web application vulnerability assessments, and plans and reports related to addressing identified web application vulnerabilities. We also interviewed Central Services' staff involved in web application security processes.

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 June 30, 2018, and Central Services' actions up to that date. We found that Central Services had implemented two of the four recommendations.

3.1 Tracking Information about Web Applications

We recommended that the Ministry of Central Services document key information about all ministry web applications that are subject to its security policy. (2016 Report – Volume 1; Public Accounts Committee agreement January 11, 2017)

Status – Implemented

Since 2016, Central Services compiled a list (i.e., inventory) of existing ministry web applications. It began maintaining details on web applications in an IT system.

Central Services determined the initial information it required to manage web applications. This included who owns the application, where the application is located, and the server on which the application resides.

Central Services compiled a spreadsheet of existing web applications that it manages on behalf of ministries. This spreadsheet lists over 460 web applications.

In addition, in 2017, Central Services began tracking all IT assets it manages on behalf of ministries, including web applications, in a central IT system. Central Services has processes for maintaining the integrity of the data (e.g., validating data entered, recording decommissioned IT assets timely) in this central IT system.[2]

Good security practices include maintaining key information about applications.

3.2 Web Applications Routinely Analyzed

We recommended that the Ministry of Central Services require routine analysis of web application vulnerabilities to monitor compliance with its security policy. (2016 Report – Volume 1; Public Accounts Committee agreement January 11, 2017)

Status – Implemented

[2] Decommissioned assets include servers or applications withdrawn from service.

Starting in late 2017, Central Services completed monthly assessments of ministry web applications to identify security vulnerabilities. [3]

Central Services used an established scanning tool to complete the vulnerability assessments. The tool rated vulnerabilities identified by level of security risk posed (high, moderate, low risk).

Routine analysis of web applications helps to identify vulnerabilities on a timely basis.

3.3 Guidance and Work to Prioritize and Address Web Application Vulnerabilities Evolving

We recommended the 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; Public Accounts Committee agreement January 11, 2017)

Status – Partially Implemented

We recommended that the Ministry of Central Services work with the ministries to address identified higher-risk web application vulnerabilities. (2016 Report – Volume 1; Public Accounts Committee agreement January 11, 2017)

Status – Partially Implemented

Central Services had appropriate guidance to support the development of secure web applications, but it was not always followed. Its guidance for maintaining security of web applications was still evolving.

Guidance in Place for Developing Secure Web Applications but Not Always Followed

Since 2016, Central Services developed guidance to support secure development of web applications but did not always follow it.

Central Services developed application security coding guidelines that include leading security industry practices. For example, guidelines required web application developers to avoid common security issues identified by the security industry (e.g., OWASP Top 10 Most Critical Web Application Security Risks).[4] The coding guidelines provided in-depth details on topics such as restricting access, encrypting data, keeping coding simple, and checking input from external users.

We found that Central Services' staff were aware of and considered the guidance when developing new web applications.

In 2017, Central Services developed a draft web application security policy. It requires security assessments for new web applications or for web applications undergoing

[3] Security vulnerabilities are weaknesses in web applications that attackers can use to see sensitive information (e.g., credit card, banking, birthdate information) while it is being processed by the web application (i.e., data in transit) or gain access to data stored by the web applications or other applications in the same network(s). In addition, attackers can exploit weaknesses in web applications to put systems and data belonging to public users at risk.

[4] OWASP is an international not-for-profit organization focused on improving the security of software.

significant change, before putting the new or changed application into use. Central Services did not always follow its requirements.

For a new web application we examined, Central Services did not complete the security assessment until eight weeks after it put the web application into use. As a result, for the high-risk vulnerability found, Central Services did not assess the security impact to the data centre or the public users who enter sensitive information into the new website.

Not assessing new web applications for potential higher-risk vulnerabilities prior to implementation increases the risk that the application could be compromised, and sensitive data lost or inappropriately accessed.

Better Guidance for Prioritizing and Addressing Web Application Vulnerabilities Needed

While Central Services began monthly web application security assessments, it did not have approved guidance that outlines the process for compiling and prioritizing identified vulnerabilities. Without prioritization guidance, Central Services may not be focusing on higher-risk vulnerabilities first.

Central Services' draft web application security policy requires routine security assessments to monitor for new vulnerabilities over time. We expected the policy would outline that higher-risk web applications should be assessed more frequently than lower-risk ones.

As previously stated, Central Services completed monthly assessments of all existing ministry web applications to identify security vulnerabilities in late 2017. Management advised us it did not use a risk-based approach to determine which web applications to assess due to the extensive amount of existing and advancing vulnerabilities that require continuous assessment.

The monthly assessments identified an extensive amount of vulnerabilities on a number of existing web applications. These vulnerabilities increase the risk of attacks causing unauthorized access to or unavailability of ministry IT systems and data.

For 13 web application vulnerability assessments we reviewed, Central Services had identified 67 high-risk and 85 medium-risk vulnerabilities. Results varied by web application, with one application having 58 high-risk vulnerabilities, and three others having no vulnerabilities. Central Services was in the early stages of working with the web application owner to address the 58 high-risk vulnerabilities.

Central Services also began working with web application owners (ministries) to address other vulnerabilities found through its assessments. We found that Central Services had not compiled or prioritized the web applications with identified higher-risk vulnerabilities to make sure higher-risk vulnerabilities are addressed within an appropriate timeframe. Rather it used informal prioritization processes to plan work to address web applications with higher-risk vulnerabilities. At June 30, 2018, Central Services continued to develop plans to address higher-risk vulnerabilities, but had significant work remaining.

Compiling, prioritizing, and addressing higher-risk vulnerabilities reduces the risk that ministry web applications can be compromised, and sensitive data lost or inappropriately accessed.