# Service Alberta—Protecting Information Assets Follow-up

## Summary

The Government of Alberta uses a variety of information technology systems to provide programs and services, and host and process personal information.

We audited the security of the government and made 11 recommendations to the ministries of Executive Council, Service Alberta and Infrastructure in our *October 2008 Report,* in three areas of IT security:

- secure development, operation and use of web applications
- security of wireless access to systems
- physical security and environmental protection of data in data facilities

In our *October 2010 Report,* we found that Service Alberta had implemented two of our IT security recommendations and was working on the other nine.

### What we examined

We assessed the work Service Alberta did to develop, implement, communicate and monitor the 10 IT security directives. We also examined the policies, procedures and other completed and ongoing work to communicate and operationalize these directives.

### What we found

We followed up on these recommendations in 2012 and found that Service Alberta had implemented eight of the original 11 IT security recommendations. We also found that Service Alberta cannot fully implement the three remaining recommendations because it lacks the authority and responsibility for overseeing IT security for certain government entities. Therefore, we stopped our audit of Service Alberta's implementation of those recommendations.

Instead, we make a new recommendation that the Government of Alberta's Executive Council (see page 62) to:

- assess the risks to public information assets throughout the government
- determine if the government has adequate IT security policies, standards and controls to mitigate risks
- determine who is responsible and accountable to ensure that public information assets are adequately protected

### Why this is important to Albertans

Albertans need to be able to access online programs and services, and obtain accurate information when needed. Albertans also need to know that the IT systems the government and publicly funded entities use are secure and available when needed and that they protect personal and government information from unauthorized use.

## Findings and recommendations

### Central security office—changed circumstances

**Background**

In our *October 2008 Report* (page 53), we recommended that Executive Council immediately establish a central security office to oversee (develop, communicate, implement, monitor and enforce) all aspects of information security for organizations using the government's shared information technology infrastructure.

### Our audit findings

Executive Council, in response to our recommendation, stated Service Alberta has the mandate to establish a central security office to oversee all aspects of infornation security for the government's shared technology infrastructure.

The Corporate Information Security Office developed and communicated 10 Information security management directives. These 10 directives were approved by the Corporate Chief Information Officer on February 5, 2010. We found that the 10 directives were based on internationally recognized standards that would reasonably protect government information assets if properly implemented and consistently followed.

However, we were unable to obtain sufficient evidence that:

- departments followed the security directives
- someone is responsible and accountable to monitor and ensure that the security directives are followed throughout government

Service Alberta considers this recommendation implemented. We found that Service Alberta did everything it believed it had the ability and authority to do. We will no longer assess Service Alberta's implementation of this recommendation. We make a new recommendation to the Government of Alberta's Executive Council (see page 62) to assess the risk to public information assets throughout the government in lieu of Service Alberta being able to set standards or monitor for compliance.

## Develop and maintain detailed policies and standards to build and operate secure web applications—implemented

### Background

Service Alberta implemented this recommendation in 2010 and we reported this as implemented in our *October 2010 Report* (page 78).

### Our audit findings

Service Alberta implemented this by working with all ministries through the CIO Council to develop, implement and communicate its 10 IT security directives.

## Develop standards and policies to ensure web applications are built to required standards (repeated in 2010)—changed circumstances

### Background

We previously recommended that Service Alberta, in conjunction with all ministries and through the CIO Council, develop and implement well-designed and effective controls to ensure all Government of Alberta web applications consistently meet all security standards and requirements (*October 2008 Report,* no. 5—page 66).

### Our audit findings

We obtained and reviewed the documentation and the process Service Alberta used to develop, implement and communicate IT security standards.

However, Service Alberta does not have the ability or authority to implement controls to monitor and enforce those security standards on Government of Alberta web applications. Therefore, the final part of the recommendation, to ensure those standards are consistently met throughout government, is not being done. Although certain departments have a process to comply with the security standards, the government as a whole does not know if all web applications that process and host government information and that of Albertans' are secured.

We will no longer assess Service Alberta's implementation of this recommendation. We make a new recommendation to the Government of Alberta's Executive Council (see page 62) to assess the risk to government information assets of Service Alberta being unable to fully implement it.

## Review and improve the Government of Alberta's shared computing infrastructure policies, procedures and standards—changed circumstances

### Background

We previously recommended that Service Alberta work with all ministries and through the CIO Council, to develop and implement security policies, procedures, standards and well-designed control activities for the Government of Alberta's shared computing network (*October 2008 Report,* page 68).

### Our audit findings

We obtained and reviewed the documentation and process Service Alberta used to develop, implement and communicate IT security standards.

However, Service Alberta also told us that it does not have the ability or authority to implement controls to monitor and enforce those security standards. We confirmed that Service Alberta implemented a system and process to monitor for security issues and vulnerabilities where it can, and informs the owners when security issues are identified. However, Service Alberta cannot take further action on security issues when those resources are not under its direct control.

Therefore, the final part of the recommendation, to ensure those standards are consistently met, is not being done. Although departments work with Service Alberta to remediate security issues in zones 2 to 4 (see diagram—page 61), Service Alberta does not have the authority to ensure that departments remediate the security issues promptly. Further, as Service Alberta has even less control over devices in zone 1, there is less ability for Service Alberta to monitor systems and notify their owners of security issues.

We will no longer assess Service Alberta's implementation of this recommendation. We make a new recommendation to the Government of Alberta's Executive Council (see page 62) to assess the risk to public information assets throughout the government.

## Wireless policies and standards—implemented

### Background

In our *October 2008 Report* (page 75), we recommended that Service Alberta, in conjunction with all ministries and through the CIO Council, update its existing wireless local area network access security policy to improve the guidance to departments for deploying and securing wireless network access points.

### Our audit findings

Service Alberta implemented this recommendation by developing and implementing two security directives that provide standards and guidance to departments to deploy and secure wireless network access points.

## Device configurations—implemented

### Background

In our *October 2008 Report* (page 76), we recommended that Service Alberta, in conjunction with all ministries and through the CIO Council, review the configuration of laptops, and approve policies to prevent laptops from inadvertently exposing the government's computer environment to security risks.

### Our audit findings

Service Alberta implemented this recommendation by developing and implementing a security directive requiring departments to implement appropriate controls to mitigate security risks associated with the use of portable computing devices such as laptops or personal digital assistants.

Further, through its service provider, Service Alberta implemented standards for security and encryption that are mandatory on laptops issued through its central services.

## Ongoing monitoring and surveillance—implemented

### Background

In our *October 2008 Report* (no. 7—page 77), we recommended that Service Alberta, in conjunction with all ministries and through the CIO Council, update network surveillance methods to detect and investigate the presence of unauthorized wireless access points within the Government of Alberta.

### Our audit findings

Service Alberta implemented technical systems and associated processes to monitor for security issues at the perimeter and throughout the government's shared computing environment. Service Alberta also developed standards and procedures to look for and assess risks to the government through wireless access points. Service Alberta then conducted a security assessment on selected departments and did not find any significant issues.

## Physical and environmental security recommendations

The next three recommendations are similar in nature. We relied on the same or similar documentation and evidence to confirm that they were implemented. Therefore, we document the individual recommendations and afterwards the combined audit findings we used for all three.

## Backup power supplies—implemented

### Background

In our *October 2008 Report,* (page 85), we recommended that Service Alberta, work in conjunction with all ministries and through the CIO Council, to ensure that ministries that use data facilities ensure that connected computer equipment has a sufficient redundant power supply.

## Physical security—implemented

### Background

In our *October 2008 Report* (page 87), we recommended that Service Alberta work with the Ministry of Infrastructure and in conjunction with all ministries and through the CIO Council, to improve:

- physical security controls at data facilities
- logging of access to data facilities by implementing effective controls to track access

## Environmental security—implemented

### Background

In our *October 2008 Report* (page 89), we recommended that Service Alberta work with ministries to improve the environmental security controls at shared data facilities.

## Our combined audit findings for the physical and environmental security recommendations

Service Alberta and the Ministry of Infrastructure developed and implemented physical and environmental standards through a security directive and standards for Alberta's shared data facilities (SDF). They also developed and implemented additional policies, procedures and standards to support the two main documents.

In 2010, we obtained and reviewed the gap analysis of physical and environmental security needs for server rooms. We also reviewed the plan—based on the risk to the systems and available resources to remediate those security gaps. In 2012, we found that the high-risk gaps identified in 2010 for SDFs are now remediated. We also obtained evidence that Service Alberta is monitoring compliance with the security standards in the SDFs and works with Infrastructure to remediate issues when they are identified through ongoing monitoring or annual self-audits.

Although sufficient work was completed to find this recommendation implemented, we will continue to follow up on Service Alberta and Infrastructure's work to remediate lower risk issues in SDFs and in other locations around Alberta that host government servers and network computing devices.