OFFICE OF THE
Auditor General
of British Columbia

Audit at a glance

Why we did this audit

- Twenty times more British Columbia government employees have been teleworking since the COVID-19 pandemic began.
- To do their work, employees and contractors remotely access government data, some of which is sensitive.
- Teleworking provides many benefits, but also exposes government data to increased risk that must be managed.

Objective

To determine if the Office of the Chief Information Officer (OCIO) has established processes and practices to effectively manage cybersecurity risk to government data in the telework environment.

Audit period:

July 2021 to February 2022

Conclusion

The OCIO has established processes and practices to effectively manage cybersecurity risk to government data in the telework environment.

We made one recommendation on detecting and responding to the use of devices not managed by government.

The ministry has accepted this recommendation.

What we found

Planning, governance, and strategic activities

In the telework environment the OCIO:

- uses an established risk assessment framework to evaluate cybersecurity risk to government data.
- has implemented and maintains policies, procedures, and standards to manage cybersecurity risk.

Data protection

The OCIO:

- protects government data transmitted to and from telework devices.
- protects government data stored on telework devices provided by government.
- prohibits the use of personal devices for teleworking but is unable to detect whether these devices are being used and if government data is stored on them.

RECOMMENDATION 1

Training and awareness

- The OCIO provides cybersecurity training and guidance for teleworkers to protect government data.
- 92% of public service employees have completed mandatory data security and privacy training.
- The OCIO assesses cybersecurity awareness and updates training and guidance for teleworkers.

OFFICE OF THE
Auditor General
of British Columbia

Audit at a glance *(continued)*

After reading the report, you may want to ask the following questions of government:

1. *What more could the OCIO do to protect government data accessed by teleworkers?*
2. *What are ministries responsible for when it comes to protecting government data?*
3. *How will the OCIO detect and respond to the use of prohibited personal devices?*