Office of the
Privacy Commissioner
of Canada

THE PROTECTION OF PERSONAL INFORMATION IN WIRELESS ENVIRONMENTS: AN EXAMINATION OF SELECTED FEDERAL INSTITUTIONS

Audit Report of the
Privacy Commissioner of Canada

Section 37 of the *Privacy Act*

FINAL REPORT

2010

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 947-1698, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190
Follow us on Twitter: @privacyprivee

Cat. No. IP54-33/2010
ISBN 978-1-100-52313-2

This publication is also available on our Web site at **www.priv.gc.ca**.

Table of Contents

Main Points

WHAT WE EXAMINED

Five organizations were selected for examination. The audit entities are: Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada. The selection was based on the extent to which these entities use wireless technologies to transmit and store personal information, the number of wireless access points to their wireless network(s), and the number of employees who have been issued portable wireless devices.

We reviewed their policies, procedures and practices for managing smartphones, cellular telephones and wireless (Wi-Fi) networks. We examined whether the audit entities have assessed the threats and risks of the wireless technologies and have implemented measures to mitigate these risks. We looked at the controls in place to protect personal information managed within a wireless environment, including the use of passwords and encryption and restrictions on the use of PIN-to-PIN messaging.

We also tested surplus wireless devices (smart and cellular phones) and scanned for wireless access points within or immediately surrounding the premises occupied by the audit entities.

WHY THIS ISSUE IS IMPORTANT

Wireless technology allows hardware devices to communicate using radio frequencies to transmit data, rather than physical cable connections used within a controlled wired environment. The wireless transmission of data is an inherently open method of communication.

Smartphones have been issued to thousands of federal public servants. The portability of these devices allows users to access and discuss confidential information while waiting in line at a bank machine, sitting in the departure lounge of an airport, or travelling to and from home on public transit. Files from a desktop computer or a corporate network can be transferred to and stored in these devices. By extension, they have the capacity to retain vast amounts of personal information. The inappropriate use, theft or loss of these devices may potentially result in an exposure of data.

The entities that we examined deliver services and programs that Canadians depend on. The delivery of these services and programs requires the use of sensitive personal information, which could include: information from those seeking assistance under housing programs administered by CMHC; information on individuals incarcerated for a period of two years or more; health care data on individuals residing in approximately 200 First Nations communities; recipients of Canada Pension, Old Age Security and Employment Insurance benefits; and information on First Nations, Inuit and Métis peoples.

These entities have an obligation to ensure that they implement technical, physical and administrative safeguards to protect the integrity and security of personal information that they transmit and store within wireless environments.

WHAT WE FOUND

The Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada have policies, procedures and processes for managing personal information transmitted to and stored within their wireless environments. However, there are weaknesses that need to be addressed.

While various security measures are in place to protect wireless (Wi-Fi) networks and portable devices, none of the entities we audited had fully assessed the threats and risks inherent to wireless technologies. In the absence of such analyses, the audit entities cannot demonstrate that all material risks have been identified and appropriately managed.

Policy and procedural controls need to be strengthened to ensure that wireless devices do not become the source of a data breach. Only three of the five audit entities have implemented strong password protection protocols for smartphones. None of the entities have a requirement to encrypt data stored in the memory of the devices, and four of the five entities do not have documented procedures to mitigate the risk of a data breach resulting from a lost or stolen device.

The portability of wireless devices allows users to conduct business in public areas. This presents a risk that personal information may be inadvertently exposed to bystanders. The risk of this occurring can be minimized with appropriate guidance and training. With one exception, we found that the entities do not, as a general practice, educate wireless users on how to use the devices in a manner that protects privacy.

Communications Security Establishment Canada (CSEC) is Canada's national cryptologic agency. CSEC's mandate includes providing advice and guidance to assist federal departments and agencies secure their electronic systems and networks. Of the Wi-Fi networks that we examined, we found that the encryption levels varied among the four audit entities that use the technology. Three of the entities have implemented their Wi-Fi networks with encryption levels that meet those recommended by CSEC.

PIN-to-PIN messaging is a direct communication between two smartphones that circumvents an organization's corporate server. Given the security vulnerabilities of this type of communication, CSEC has recommended that departments refrain from using the technology and disable the functionality on smartphones. In the event that a department has a specific requirement for PIN-to-PIN messaging (e.g. emergency response), CSEC recommends that a clear policy on its use be put in place and supplementary measures be employed to protect the privacy and confidentiality of such communications.

We found that contrary to the Communications Security Establishment Canada recommendation, all audit entities allow PIN-to-PIN messaging. Further, none of the entities were able to demonstrate that they have implemented measures to address the security issues surrounding the use of this communication method.

Finally, we noted weaknesses surrounding the management of surplus wireless devices. Departments and agencies have sole responsibility for preventing the unauthorized release of information contained in surplus assets. Four of the five entities could not demonstrate that all smartphones and cellular telephones are cleansed (wiped) of data prior to being sent for disposal.

The Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada have responded. Their responses are found in the Appendix to this report.

Introduction

BACKGROUND

1. The use of wireless communication has grown dramatically. Wireless technologies include Wi-Fi networks and smartphones (such as the BlackBerry). These devices provide computing power and connectivity, allowing users access to information where previously it was not available.

2. The processing and storage capabilities of wireless devices make them attractive and valuable tools for service and program delivery. Files and applications traditionally found on desktop personal computers can be processed by portable devices and data from a corporate network can be transferred to these devices with relative ease.

3. Whether used for data transmission or voice communication, wireless technologies bring flexibility and convenience to public servants on the move. While these technologies offer many benefits, they may also put personal information at risk.

4. Five organizations were selected for audit examination. The entities are: Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada.

5. These entities deliver programs and services that require the use of sensitive personal information. The Canada Mortgage and Housing Corporation requires access to information in order to provide assistance to Canadians seeking access to safe, affordable housing. Correctional Service of Canada retains information on individuals incarcerated for a period of two years or more. As the primary health care provider for approximately 200 First Nations communities, Health Canada maintains health care files on thousands of individuals. Human Resources and Skills Development Canada manages personal information on recipients of Canada Pension, Old Age Security and Employment Insurance benefits. Indian and Northern Affairs Canada support First Nations, Inuit and Métis peoples in their efforts to improve their social and economic well being.

FOCUS OF THE AUDIT

6. The objective of the audit was to determine whether the selected entities have adequate controls – including policies, procedures and processes – to protect personal information transmitted and stored within wireless environments. We examined the security frameworks surrounding wireless networking and the use of portable wireless devices.

7. The audit did not include an examination of the entities' overall personal information handling practices or their overarching Information Technology Security infrastructures. Additional details regarding the audit objective, scope, approach, and criteria are available in the **About the Audit** section of this report.

Observations and Recommendations

POLICY AND PROCEDURAL CONTROLS

8. Treasury Board's Policy on Government Security and its related standards prescribe safeguards to protect and preserve the confidentiality and integrity of government assets, including personal information. These instruments set out baseline (mandatory) security requirements.

9. Federal entities are required to conduct their own assessments to determine whether safeguards above baseline levels specified by the policy are necessary. The policy also calls for ongoing monitoring of the threat environment to ensure appropriate security measures are maintained.

10. We expected that the Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada have

    - assessed the threats and risks of their wireless technologies (smartphones and Wi-Fi networks),
    - provided guidance to staff on the acceptable use of smart and cellular phones,
    - set out a process to address lost or stolen wireless devices,
    - implemented security requirements such as the use of passwords and encryption to protect personal information within wireless environments,
    - ensured that the use of PIN-to-PIN messaging was consistent with guidance issued by Communications Security Establishment Canada, and
    - established procedures for the secure disposal of surplus smart and cellular phones.

Risks and threats have not been formally assessed

11. If wireless technologies are not configured with proper safeguards, they could potentially allow unfettered access to an organization's network and data. A Threat and Risk Assessment (TRA) defines the threat environment, evaluates the associated risks and recommends mitigating actions to address identified vulnerabilities. The assessment also validates whether the minimum standards required under Treasury Board policy are appropriate for the type of information being transmitted and stored within a wireless environment.

12. While various levels of security are in place to protect wireless networks and devices, we found that the Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, and Indian and Northern Affairs Canada have not conducted TRAs on their wireless networks. We found that Correctional Service of Canada had performed a Vulnerability Assessment on its Wi-Fi installation. While Treasury Board policy recognizes that there are certain overlaps

with the two types of assessments, a Vulnerability Assessment is not designed to identify all threats and risks associated with a given technology or environment. In the absence of such analyses, the entities could not demonstrate that existing controls on their wireless networks and smartphones are sufficient. Human Resources and Skills Development Canada was in the process of completing a TRA at the time of our audit.

13. RECOMMENDATION

Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, and Indian and Northern Affairs Canada should assess the security and privacy risks associated with wireless networks and smartphones by undertaking a Threat and Risk Assessment.

Limited guidance is provided on how to protect personal information while using smartphones

14. The portability of wireless devices allows users to conduct business while on the go. Discussions that traditionally occurred behind office doors may now take place in public areas. This presents a risk that personal information may be inadvertently exposed to bystanders.

15. We expected to find that the audited entities have provided guidance to employees to ensure that wireless devices are used in a manner that respects privacy. We surveyed the entities to determine whether they sensitize employees to the risks associated with the use of smartphones. We then verified the responses we received through interviews. We also examined the agreements users are required to sign when a smart phone is issued to them.

16. With one exception, none of the entities were able to demonstrate that smart phone users had received privacy specific training to address issues such as measures to protect data stored in wireless devices and the implications of using the technology in public areas.

17. The Canada Mortgage and Housing Corporation has implemented various training initiatives, including presentations and security orientation guides for various internal audiences. These address wireless user responsibilities, the types of information that can be transmitted, solutions to safeguard the devices and wireless security issues in significant detail.

18. We also noted that Human Resources and Skills Development Canada had an awareness campaign to remind employees that discussions—involving personal information—should not occur in public areas where the risk of being overheard is high.

19. The agreement that a wireless user signs with his/her organization focuses on administrative and security matters regarding the operation of the cellular or smart phone. None of the agreements contain provisions on the users' responsibility to operate the device in a manner that protects privacy.

20. RECOMMENDATION

Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should ensure that employees are made aware of the privacy risks inherent to the use of smartphones and provide guidance to mitigate these risks.

Processes to address lost and stolen smartphones have not been formalized

21. Promptly responding to a lost or stolen wireless device will minimize the risk of personal information being compromised. We expected the audit entities to have documented procedures to deal with such occurrences.

22. We found that practices varied between the entities and in some cases within the audit entity itself. While users are instructed to report the loss or theft of a smart phone, only one entity – the Canada Mortgage and Housing Corporation (CMHC) – was able to provide documented procedures outlining the steps that should be taken to mitigate the risk of a data breach. The process includes erasing the data, disabling the device and removing the wireless user from the server. For each lost or stolen smart phone, CMHC's Security and Risk Management Group conducts an investigation, confirms that the data has been erased and the device has been disabled, and reports the results monthly to the President of CMHC. However, we noted that the Corporation was unable to demonstrate that this process is followed on a consistent basis. CMHC indicated that it would review its procedures and tools to ensure the residual risks, if any, are properly mitigated.

23. In the absence of documented procedures and assurance that they are consistently applied, there is a risk that personal information could be exposed. For example, we were informed that there have been occasions when a telecommunication service provider was notified of the loss or theft before a wipe command was sent to the wireless device. Once the service to a smart phone is deactivated, its capacity to transmit or receive a message is disabled. Consequently, the device cannot be wiped and any data—including personal information—will remain in it.

24. RECOMMENDATION

Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should establish documented procedures for responding to incidents of lost or stolen wireless devices.

SAFEGUARDS SURROUNDING PERSONAL INFORMATION

Lack of strong passwords and the absence of encryption on smartphones present a risk to privacy

25. Smartphones are widely used within the federal government. They are configured to work with a corporate e-mail account and have the capacity to store thousands of e-mails and attachments. To protect privacy and reduce the risk of an unauthorized disclosure of personal information, we expected audit entities to have clear policies establishing baseline security requirements for wireless devices.

26. The use of passwords and encryption are key safeguards in protecting personal information transmitted to and stored in smartphones. Such safeguards ensure that only those authorized to access data can do so. We examined how the audit entities configured their enterprise servers for smartphones. We also interviewed information technology personnel and security managers.

27. Communications Security Establishment Canada (CSEC) recommends the use of strong passwords for all government business. A strong password requires a mixture of at least eight characters that includes upper and lower case letters, numbers and symbols.

28. We found that Health Canada, Human Resources and Skills Development Canada and Indian and Northern Affairs Canada have implemented strong password protocols for smartphones. Correctional Service of Canada requires the use of a password to protect its smartphones; however, it does not specify that it contain the elements of a strong password. While the Canada Mortgage and Housing Corporation strongly encourages the use of passwords in various policies and communications, the decision to activate the password feature is left to the wireless user.

29. Encryption is the process of transforming information to make it unreadable except to those possessing what is referred to as a "key". Encryption is commonly used to protect information within various types of systems. None of the audited entities require data to be encrypted in the memory of wireless devices. Encrypting data provides an additional layer of security to reduce the risk of unauthorized access to data in the event that a device is lost or stolen.

30. The absence of strong passwords and encryption present a significant privacy risk. The consequences could be severe given that smartphones may retain significant amounts of personal information.

31. RECOMMENDATION

Canada Mortgage and Housing Corporation and Correctional Service of Canada should require the use of strong passwords for their smartphones.

32. RECOMMENDATION

Canada Mortgage and Housing Corporation, Correctional Service Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should ensure that data stored in smartphones is encrypted.

PIN-to-PIN messaging is vulnerable to interception

33. PIN-to-PIN messaging – also known to as Peer-to-Peer messaging – is a direct communication between smartphones that function on the BlackBerry network. Messages are addressed to a "PIN" (unique to each smart phone device) rather than an e-mail address. The messages are routed directly over the host telecommunication carrier's network, thereby bypassing an organization's corporate servers.

34. PIN-to-PIN messages can be easily intercepted with equipment that is both inexpensive and readily accessible. Information Technology Security Bulletins issued by CSEC in October 2008 and January 2010 highlight the non-secure nature of this method of communication. The bulletins further state that PIN-to-PIN messaging is not suitable for exchanging sensitive information and recommends that departments and agencies refrain from using this technology. In the event that an institution has a specific requirement for PIN-to-PIN messaging (e.g. emergency response), CSEC recommends that a clear policy on its use be put in place and supplementary measures be employed to protect the privacy and confidentiality of such communications. We examined how smartphones were configured to determine whether the audit entities follow CSEC guidance.

35. We found that contrary to CSEC's recommendation, all of the audit entities allow the use of PIN-to-PIN messaging. Further, none of the entities were able to demonstrate that they have implemented measures to address the security issues surrounding the use of this communication method.

36. RECOMMENDATION

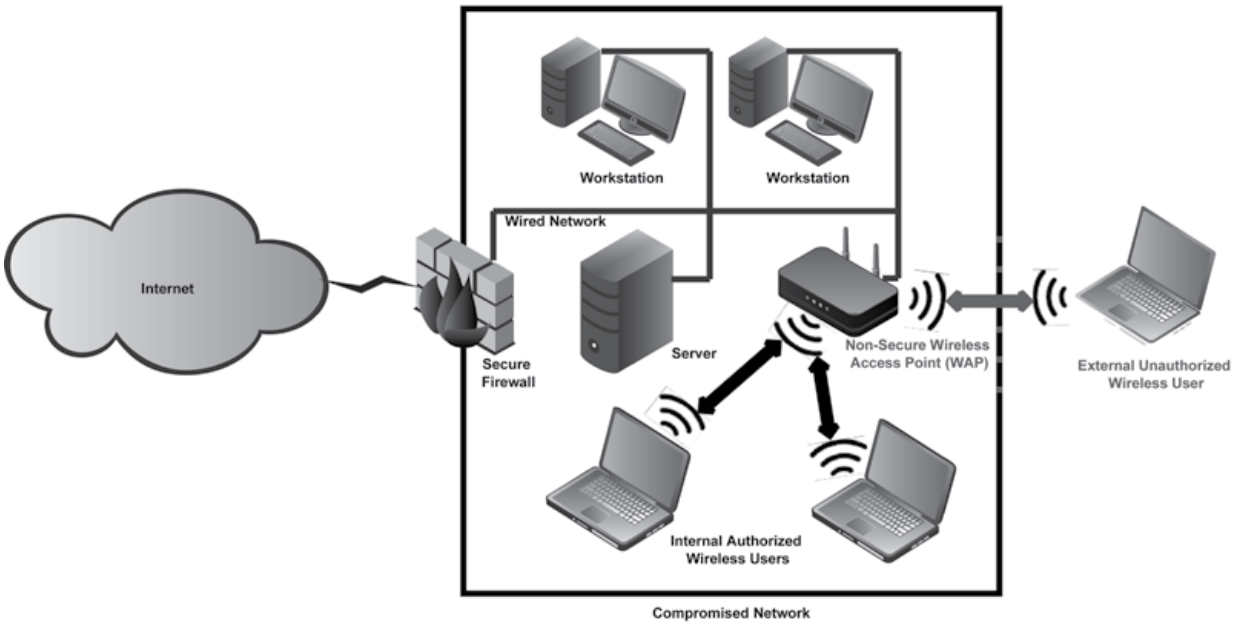
Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should ensure that the use of PIN-to-PIN messaging is consistent with the guidance issued by Communications Security Establishment Canada.

Wireless access points have varying levels of protection

37. Wireless computing (Wi-Fi) is increasingly being used by businesses, governments and individuals. Wi-Fi networks use radio waves to transmit data to wireless-enabled devices (e.g. laptops).

38. Wireless networks can be exploited by individuals who, with specially equipped laptops, detect signals from wireless transmissions. This allows the attacker to identify access points with weak or no security encryption. Once this vulnerability is detected, a variety of attacks may be carried out. Such attacks may include capturing, modifying or deleting messages or utilizing an authorized user's privileges to gain access to a system. We therefore expected the entities' Wi-Fi networks to be protected with strong security encryption.

A rogue or unsecure wireless access point allows unauthorized external access to a corporate network by bypassing the security provided by the firewall.



Source: Compiled by the Office of the Privacy Commissioner of Canada

39. As part of our testing we monitored the airspace within or immediately surrounding the premises occupied by the audit entities. This monitoring activity is referred to as war driving. We examined the transport details of the transmissions to determine their origin and encryption level; we did not review the content of the communications.

40. Human Resources and Skills Development Canada does not have any Wi-Fi installations that we were able to detect.

41. The encryption levels used to mitigate the threat of data exposure varied among the remaining four audit entities. We found that the Wi-Fi networks at the Canada Mortgage and Housing Corporation and Indian and Northern Affairs Canada have encryption levels recommended by CSEC. There is limited use of Wi-Fi technology at Correctional Service Canada. Based on our review of its configuration, we are satisfied that appropriate measures are in place to protect data transmissions over the network.

42. Health Canada uses Wi-Fi computing in certain remote locations. Although we did not verify the encryption levels at these locations, departmental officials informed us that the security encryption used does not meet the level recommended by CSEC.

43. RECOMMENDATION

Health Canada should review its wireless networks and ensure that the access points are set with security encryption recommended by Communications Security Establishment Canada.

DISPOSAL PRACTICES

Entities are generally storing surplus wireless devices securely

44. Federal entities are required to ensure that personal information is securely stored pending its disposal. They must also ensure that information is disposed of in a manner that does not compromise privacy.

45. We examined the processes staff follow to dispose of wireless devices and conducted site visits at each of the audit entities' head and regional offices where surplus smart and cellular phones are collected and stored. We also interviewed managers and employees responsible for ensuring that data is deleted from the devices.

46. The audit entities are collectively storing thousands of the surplus wireless devices. The storage methods to secure the devices varied. With the exception of Human Resources and Skills Development Canada (HRSDC), all of the entities have implemented secure measures to protect these assets. We found that surplus wireless devices are stored in locked filing cabinets or secure rooms, with limited access to both.

47. We did note that at one HRSDC regional office, surplus smart and cellular phones were stored in an unlocked filing cabinet in an area accessible to all staff. We tested a sample of the devices in this area and found a number that contained data.

48. RECOMMENDATION

Human Resources and Skills Development Canada should ensure that all of its surplus wireless devices are stored in secure areas.

Data is not wiped on all surplus smartphones and cellular telephones

49. Federal departments and agencies generally dispose of surplus assets through Public Works and Government Services Canada – Crown Assets Distribution (CAD), the organization responsible for the sale, distribution, disposal and re-use of surplus federal goods.

50. Surplus wireless devices can represent a significant privacy risk if they are not cleansed (wiped) of data prior to being disposed of, regardless of the disposal method used (i.e. physical destruction or transfer to CAD for public auction). It is the responsibility of the originating (disposing) department or agency to ensure that this is done.

51. We tested a sample of surplus wireless devices from all audit entities with the exception of the Canada Mortgage and Housing Corporation. We asked the Corporation to provide records (e.g. control sheets, logs) to demonstrate that surplus devices were wiped. While the Corporation has a process for wiping data on surplus phones, it does not maintain checklists to verify that all steps in the process have been completed in all circumstances.

52. We found that all surplus smart and cellular phones at Indian and Northern Affairs Canada were wiped of data. This was not the case at Correctional Service of Canada, Health Canada, and Human Resources and Skills Development Canada where we found data residing on a number of surplus devices that were destined for disposal.

53. RECOMMENDATION

Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, and Human Resources and Skills Development Canada should establish control mechanisms to provide assurance that data stored on surplus wireless devices is purged prior to disposal.

Conclusion

54. While various security measures are in place to protect wireless (Wi-Fi) networks and portable devices, none of the audited entities have fully assessed the threats and risks inherent with the use of wireless technologies. In the absence of such analyses, there is no assurance that all material risks have been identified and appropriately mitigated.

55. Of the Wi-Fi networks we examined, we found that the encryption levels varied among the four entities that have deployed the technology. Three of the four entities have implemented security encryption that meets the level recommended by Communications Security Establishment Canada. The remaining department utilizes a weaker form of encryption.

56. Additional safeguards are needed to ensure that smartphones do not become the source of a data breach. Only three of the five entities have implemented a strong password protection requirement for their smartphones, and none of the entities require data to be encrypted on these devices.

57. Existing policies surrounding wireless devices lack key elements – including restrictions on the use of PIN-to-PIN messaging – and four of the five entities lack documented procedures to mitigate the risk of a data exposure resulting from a lost or stolen wireless device. Furthermore, with one exception the entities do not, as a general practice, educate users on the privacy risks associated with wireless devices or how to use them in a manner that respects privacy.

58. Finally, current controls for managing surplus wireless devices are not adequate. Only one entity was able to demonstrate that existing measures provide assurance that data is wiped from smart and cellular phones prior to being sent for disposal.

59. The use of wireless technologies and devices to transmit and store personal data poses certain privacy risks. Based on our audit work, we concluded that the Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada need to strengthen certain policies, procedures and/or controls to further mitigate these risks.

About the Audit

AUTHORITY

Section 37 of the *Privacy Act* empowers the Privacy Commissioner to undertake compliance reviews of the manner in which government institutions manage their personal information holdings and make recommendations that the Commissioner considers appropriate.

OBJECTIVE

The objective of the audit was to determine whether the Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada have adequate controls – including policies, procedures and processes – to protect personal information transmitted and stored within wireless environments.

CRITERIA

The criteria used to conduct the audit were derived from the *Privacy Act*, relevant Treasury Board policies, Generally Accepted Privacy Practices, IT Governance Institute, Control Objectives for Information and related Technology (COBIT® 4.1) and the Information Technology Infrastructure Library (ITIL) Framework.

We expected the selected government organizations to have

- assessed the threats and risks inherent to the use of wireless technologies,
- provided guidance to staff on the acceptable use of smartphones and cellular telephones,
- established a formalized process for addressing incidents of lost or stolen wireless devices,
- implemented baseline security requirements, including the use of strong passwords and encryption, to protect personal information within a wireless environment,
- ensured that the use of PIN-to-PIN messaging was consistent with guidance issued by Communications Security Establishment Canada, and
- established procedures for the secure disposal of surplus wireless devices.

SCOPE AND APPROACH

The audit commenced with a survey of 34 government organizations to obtain an overview of wireless use within the federal government. The five organizations selected for audit examination manage significant amounts of personal information to fulfil their legislative mandates.

We interviewed staff and reviewed policies, procedures and guidelines. We also examined a sample of surplus wireless devices to determine whether they had been cleansed (wiped) of all data prior to being sent for disposal.

Finally, we monitored the wireless airspace within or immediately surrounding the premises occupied the audit entities. We obtained a legal opinion to confirm that our activity in this regard did not violate any provincial or federal laws.

Audit activities were carried out in the National Capital Region, Toronto, Montreal, Quebec City, Winnipeg, Vancouver and Abbotsford.

Our audit work was substantially completed on August 30, 2009.

AUDIT STANDARDS

The audit work was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner of Canada, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

AUDIT TEAM

Director General: Steven Morgan

Michael Fagan
Bill Wilson
Paul Zind

Appendix – List of recommendations

Risks and threats have not been formally assessed

RECOMMENDATION

Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, and Indian and Northern Affairs Canada should assess the security and privacy risks associated with wireless networks and smartphones by undertaking a Threat and Risk Assessment.

Canada Mortgage and Housing Corporation response: CMHC analyses security risks and mitigation strategies during implementation of all wireless functionality and technology. Threat and risks are reviewed on an ongoing basis and improvements are implemented as required. IT Security Policies and Security of Information Policies also include policies and guidelines on how to protect information. These policies are made available to all employees via training sessions, communication and online databases. CMHC has never experienced any issues in these areas.

Correctional Service of Canada response: Correctional Service of Canada (CSC) does not fully agree with the conclusion stating that it has not conducted Threat and Risk assessments on its wireless installations. CSC views the Wi-Fi component as an extension of its present network. A Network Threat and Risk assessment will be updated to include the Wi-Fi component based on evidence gathered in vulnerability assessments and reviews on wireless use within the department.

CSC is developing an action plan to address the smart phone component of the recommendation.

Health Canada response: Health Canada agrees that a Threat and Risk Assessment (TRA) should be performed and that Health Canada will undertake a TRA for wireless networks and smartphones.

Indian and Northern Affairs Canada response: INAC will prepare a Threat and Risk Assessment on its wireless networks, devices and smartphones to determine the security and privacy risks associated with these systems. This will include an overview of existing Threat and Risk Assessments of specific technologies as well as additional Threat and Risk Assessments of specific technologies as required. The identified risks and mitigation strategy will be presented to Senior Management.

Limited guidance is provided on how to protect personal information while using smartphones

RECOMMENDATION

Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should ensure that employees are made aware of the privacy risks inherent to the use of smartphones and provide guidance to mitigate these risks.

Correctional Service of Canada response: Correctional Service of Canada agrees with the recommendation and is working on a management action plan to address the issue.

Health Canada response: Health Canada agrees that employees should be made aware of the privacy risks inherent to the use of smartphones and will provide the necessary guidance for the mitigation of these risks. Health Canada is expanding the Wireless Device User Agreement and Policy to include the user's responsibility to operate the device in a manner that protects the privacy of individuals and departmental information. Additionally, the Wireless Policy will instruct users to restrict the use of transmissions of a non-sensitive nature and this restriction will include the protection of personal privacy. Users will be advised that they should not use their wireless devices to communicate designated information regarding employees or others.

Human Resources and Skills Development Canada response: Human Resources and Skills Development Canada accepts this recommendation. The Department will update its IT security awareness program. Further, the department will ensure employees are made aware of privacy risks when using smart phones and are provided with guidance to mitigate those risks.

Indian and Northern Affairs Canada response: It is recognized the Indian and Northern Affairs Canada (INAC) needs to develop or update policies, standards, and guidelines regarding the use of Wireless devices and to incorporate privacy concerns into these documents. The IT Security Division currently participates in the New Employee Orientation information sessions and promotes IT Security Awareness to all personnel through awareness sessions, posters, INAC Express electronic newsletter and website updates. Departmental Security and the Privacy Unit also promote awareness through multiple communications mediums. The material will need to be updated to place more emphasis on privacy matters pertinent to all forms of wireless communication.

Processes to address lost and stolen smartphones have not been formalized

RECOMMENDATION

Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should establish documented procedures for responding to incidents of lost or stolen wireless devices.

Correctional Service of Canada response: Correctional Service of Canada agrees with the recommendation and is working on a management action plan to address the issue.

Health Canada response: Health Canada agrees that employees should be made aware of the privacy risks inherent in the use of smartphones and will provide the necessary guidance for the mitigation of these risks. All new users will be requested to read and sign the updated Wireless Device User Agreement when they are first assigned a wireless device. This Agreement will also apply to existing wireless device users. The Agreement will also include procedures for responding to incidents where devices have been lost or stolen.

Human Resources and Skills Development Canada response: Human Resources and Skills Development Canada accepts this recommendation. The Department already has documented procedures in place nationally for BlackBerrys and will put a similar process in place for cellular phones to ensure standardization on a national level.

Indian and Northern Affairs Canada response: Indian and Northern Affairs Canada currently has a documented process in place for responding to incidents; however the process requires updating to include privacy concerns regarding lost or stolen wireless devices. Communication to employees regarding the incident process must occur regularly. In addition, the requirement for reporting lost or stolen devices will be incorporated into the Wireless Device Policy.

Lack of strong passwords and the absence of encryption on smartphones present a risk to privacy

RECOMMENDATION

Canada Mortgage and Housing Corporation and Correctional Service of Canada should require the use of strong passwords for their smartphones.

Canada Mortgage and Housing Corporation response: CMHC has always strongly recommended that staff use password protection on their smart phone in various internal policies and communications. On May, 26 2010, mandatory BlackBerry Password Protection and data encryption have been implemented at CMHC.

Correctional Service of Canada response: Correctional Service of Canada agrees with the recommendation and is working on a management action plan to address the issue.

RECOMMENDATION

Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should ensure that data stored in smartphones is encrypted.

Canada Mortgage and Housing Corporation response: CMHC has always strongly recommended that staff use password protection on their smart phone in various internal policies and communications. On May 26, 2010, mandatory BlackBerry Password Protection and data encryption have been implemented at CMHC.

Correctional Service of Canada response: Correctional Service of Canada agrees with the recommendation and is working on a management action plan to address the issue.

Health Canada response: Health Canada agrees that the data stored in smartphones should be encrypted. Health Canada is working with wireless vendors to develop procedures and processes to ensure that the data has been encrypted up to Communications Security Establishment Canada (CSEC) standards. Health Canada will determine the feasibility of including supplementary encryption and data protection for the BlackBerry Enterprise Server (commonly known as BES). This will allow for all Health Canada users to comply with the data protection requirements of the Government Security Policy (GSP) as well as the CSEC standards.

Human Resources and Skills Development Canada response: Human Resources and Skills Development Canada accepts this recommendation. The Department agrees that a level of risk exist with regards to the security of data stored in smart phones. The Department is willing to participate in Government of Canada wide discussions on this matter to gain a better understanding of the risk associated with data storage on these devices, and facilitate its assessment of the implications, which would lead to informed decision making.

Indian and Northern Affairs Canada response: A Risk Assessment will be conducted on the wireless technology currently in use within the Department. The results of the Risk Assessments, in conjunction with CSE-based recommendations, will drive the required encryption implementations to better safeguard sensitive information within Indian and Northern Affairs Canada.

PIN-to-PIN messaging is vulnerable to interception

RECOMMENDATION

Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, Human Resources and Skills Development Canada, and Indian and Northern Affairs Canada should ensure that the use of PIN-to-PIN messaging is consistent with the guidance issued by Communications Security Establishment Canada.

Canada Mortgage and Housing Corporation response: CMHC policies clearly communicate that PIN-to-PIN messaging should only be used in rare cases of an emergency situation as per our Business Continuity Plans.

CMHC has established a process whereby recipients of BlackBerry devices must formally acknowledge having read all associated policies, terms and conditions for the use of the device, including those related to the use of PIN-to-PIN.

Correctional Service of Canada response: Correctional Service of Canada agrees with the recommendation and is working on a management action plan to address the issue.

Health Canada response: Health Canada agrees that PIN-to-PIN messaging is inconsistent with the guidance issued by CSEC. For users with specific requirements for PIN-to-PIN messaging (e.g. emergency communications), the wireless policy will be expanded to include the use of PIN-to-PIN messaging, and supplementary measures will be used to protect the privacy and confidentiality of PIN-to-PIN messaging. The BlackBerry Enterprise Server (BES) administrator has the option to set-up an organization-specific to the PIN-to-PIN encryption key in the BES. It should be noted that this overrides the default global encryption key and limits the ability to decrypt PIN-to-PIN messages to departmental BlackBerry devices which are connected to the BES. However, this also prevents PIN-to-PIN communication with BlackBerry devices outside of the department, and may prevent emergency communications with outside organizations. Thus, use of this feature will be carefully considered for the BES administrator using the option to set-up an organization-specific PIN-to-PIN.

Human Resources and Skills Development Canada response: Human Resources and Skills Development Canada accepts this recommendation. The Department agrees that a properly defined operational requirement of PIN to PIN communications is critical for its infrastructure services and will participate in a Government of Canada wide approach that includes discussions with Communications Security Establishment Canada to clarify/define acceptable use of PIN to PIN messaging.

Indian and Northern Affairs Canada response: Indian and Northern Affairs Canada is partially compliant with CSEC guidelines on the use of BlackBerrys and PIN-to-PIN technology. The IT Security Division, in conjunction with other IM/IT stakeholders is currently completing an analysis on the use of BlackBerrys within the Department. The analysis will assess the management, technical and operational controls throughout the lifecycle of BlackBerry devices, identify the risks, and provide recommendations to mitigate the risk.

Wireless access points have varying levels of protection

RECOMMENDATION

Health Canada should review its wireless networks and ensure that the access points are set with security encryption recommended by Communications Security Establishment Canada.

Health Canada response: Health Canada agrees that a review should be undertaken of wireless networks. Health Canada will endeavour to ensure that all access points are set with security encryption as recommended by CSEC.

Entities are generally storing surplus wireless devices securely

RECOMMENDATION

Human Resources and Skills Development Canada should ensure that all of its surplus wireless devices are stored in secure areas.

Human Resources and Skills Development Canada response: Human Resources and Skills Development Canada accepts this recommendation and will update its Wireless Device Policy Directive accordingly.

Data is not wiped on all surplus smartphones and cellular telephones

RECOMMENDATION

Canada Mortgage and Housing Corporation, Correctional Service of Canada, Health Canada, and Human Resources and Skills Development Canada should establish control mechanisms to provide assurance that data stored on surplus wireless devices is purged prior to disposal.

Canada Mortgage and Housing Corporation response: CMHC follows a documented process to wipe data on surplus phones. No issues have been reported on the existing process. CMHC will include a document in each file to describe what was done.

Correctional Service of Canada response: Correctional Service of Canada agrees with the recommendation and is working on a management action plan to address the issue.

Health Canada response: Health Canada agrees that controls should be established to ensure that data stored on surplus wireless devices is purged prior to disposal. Currently Health Canada has controls in place for new Cell Phone users, a Consent Form which is obligatory, that contains detailed information including a section on Cell Phone Disposal/Return Instructions that outlines the process when returning devices.

In addition, Health Canada is currently modifying the wireless policy so that it will provide detailed instructions to the wireless user with procedures/directives to follow to ensure that data stored is wiped/purged prior to disposal.

Human Resources and Skills Development Canada response: Human Resources and Skills Development Canada accepts this recommendation. The department physically destroys its surplus wireless devices and has already taken steps to standardize the destruction process. In addition, the department will update its current Wireless Device Policy Directive and ensure the enhanced process is communicated to all involved parties.