CORRECTIONAL SERVICE CANADA

CHANGING LIVES. PROTECTING CANADIANS.

# Audit of Interception of Inmate Communications

**INTERNAL AUDIT SECTOR**

**APRIL 2021**

Correctional Service Canada | Service correctionnel Canada

Canada

# TABLE OF CONTENTS

# NOTE TO READER

The Internal Audit Sector completed a follow-up to the audit in February and March, 2020. The results of the follow-up can be found in Addendum A.

# EXECUTIVE SUMMARY

## What We Examined

The Audit of Interception of Inmate Communications was conducted as part of Correctional Service Canada's (CSC) 2017-2020 Risk-Based Audit Plan. In order to help maintain safety and security within institutions, and pursuant to requirements in the *Corrections and Conditional Release Regulations* and the *Criminal Code*, CSC can intercept inmate communications to obtain intelligence information that may assist with the prevention and management of an act that would jeopardize the security of the penitentiary or the safety of any person, providing it is the least restrictive measure available in the circumstances.

The objectives of this audit were to:

- Provide assurance that the management framework in place supports the efficient and effective achievement of communication intercept objectives; and
- Provide assurance that key activities have been implemented in compliance with requirements.

For the first objective, the audit examined whether:

- CSC guidance is complete, clear, and aligns with legislation;
- CSC provides training to support the discharge of responsibilities;
- CSC has in place the necessary equipment to intercept inmate communications; and
- CSC conducts monitoring on a regular basis and documents and reports on results to the required management level.

For the second objective, the audit examined whether:

- Reasonable grounds is adequately documented and supported by intelligence information;
- Approval to intercept is given in writing, by an individual with the appropriate authority, prior to the start of related intercept activity;
- Interception is carried out in compliance with approvals; and
- Information is appropriately secured and shared.

The audit was completed in two phases and included the framework and processes in place at the national, regional, and local levels.

Phase 1 was national in scope and included an analysis of three methods of intercepting communication: telephone; communication during the course of a visit; and mail. File review included a sample of communication intercepts that were approved and completed from January 1, 2017 – June 22, 2018 at institutions selected in three of the five regions.

Upon completion of Phase 1 in Autumn 2018, the Senior Deputy Commissioner in collaboration with the Assistant Commissioner Correctional Operations and Programs and the Regional Deputy Commissioners prepared an action plan to immediately address the most significant preliminary findings. The actions taken by management focused on the following three areas: providing updated guidance to institutions; providing training to institutional management and Security Intelligence Officers (SIO) on the legal and policy framework as well as on the voice logger; and implementing oversight and quality assurance processes at both RHQ and NHQ over authorizations to intercept.

Phase 2 was national in scope and assessed if management actions were effective in addressing the most significant issues raised through Phase 1 of the audit. Specifically, it included an assessment of reasonable grounds, approvals to intercept, and compliance with approvals. File review focused solely on the interception of telephone communication and included a sample of communication intercepts that were approved and completed from November 1, 2018 – April 12, 2019 at institutions selected in all five regions.

## Why it's Important

The audit links to CSC's corporate priority of ensuring the "safety and security of the public, victims, staff and offenders in institutions and in the community" [1], and to CSC's corporate risk that "CSC will not be able to maintain required levels of operational safety and security in institutions and in the community".[2]

CSC has been granted authority under the *Corrections and Conditional Release Act* to intercept inmate communications without receiving prior judicial authorization. Given the significance of this authority and the impact on an inmate's right to privacy, it is essential that CSC has an adequate and effective framework in place to ensure that inmate communication is intercepted in a manner consistent with legislative requirements.

## What We Found

Overall, we found that elements of a management framework were in place; however, improvements were required to help ensure that the framework supports the efficient and effective achievement of communication intercept objectives. A lack of guidance and limited training caused institutional management and SIOs to have an incomplete understanding of the legal and policy requirements for intercepting inmate communications, which resulted in significant compliance issues. Specifically, reasonable grounds were often not adequately documented and/or supported by intelligence information, authorization to intercept an inmate's communication was not always provided in writing, and communications (including privileged) were at times intercepted without approval. These compliance issues had gone largely undetected due to insufficient quality assurance over the intercept work performed by the SIOs, and a lack of monitoring and reporting activity. We also identified that intercept activity was not always well-documented, and information obtained through intercept activity was not always properly managed. In addition, we found a lack of effective safeguards to ensure that CSC was meeting its legal and policy obligations with respect to notifying inmates that their communication had been intercepted.

Through Phase 2 we found that management's actions resulted in significant improvements in compliance with key legislative and CSC policy requirements. Recommendations have been issued based on areas where continued improvement is required.

## Management Response

Management agrees with the audit findings and recommendations as presented in the audit report. Management has prepared a detailed Management Action Plan to address the issues raised in the audit and associated recommendations. The Management Action Plan is scheduled for full implementation by June 30, 2021.

[1] CSC 2018-2019 Corporate Risk Profile
[2] ibid

# ACRONYMS & ABBREVIATIONS

| | |
|---|---|
| ACCOP | Assistant Commissioner, Correctional Operations and Programs |
| ADCCO | Assistant Deputy Commissioner Correctional Operations |
| CCRA | Corrections and Conditional Release Act |
| CCRR | Corrections and Conditional Release Regulations |
| CD | Commissioners Directive |
| CORR | Compliance and Operational Risk Report |
| CSC | Correctional Services Canada |
| CSS | Corporate Services Sector |
| DW | Deputy Warden |
| ESS | Electronic Security Systems |
| FPS | Finger Print System |
| GL | Guidelines |
| IH | Institutional Head |
| IT | Information Technology |
| ITS | Inmate Telephone System |
| NHQ | National Headquarters |
| NTS | National Training Standards |
| OPI | Office of Primary Interest |
| PIN | Personal Identification Number |
| PSI | Preventive Security and Intelligence |
| RBAP | Risk-Based Audit Plan |
| RCMP | Royal Canadian Mounted Police |
| RHQ | Regional Headquarters |
| SIC | Strategic Intelligence Committee |
| SIO | Security Intelligence Officer |
| SO | Standing Order |
| TOR | Terms of Reference |
| V&C | Visits and Correspondence |

# GLOSSARY

| | |
|---|---|
| Common call list: | A list of contacts and associated information (i.e. phone number, relationship to inmate, etc.) that all inmates are permitted to make phone calls to.[3] |
| **(REDACTED)** | **(REDACTED)**[4] |
| Dynamic security: | Regular and consistent interaction with offenders and timely analysis of information and sharing through observations and communication (e.g. rapport building, training, networking, intelligence gathering and strategic analysis). Dynamic security is the action that contributes to a safe working and living environment for staff and offenders, and is a key tool to assess an offender's adjustment and stability.[5] |
| **(REDACTED)** | **(REDACTED)**[6] |
| Information life cycle: | Encompasses planning; collection, creation, receipt, and capture; organization; use and dissemination; maintenance, protection and preservation; disposition; and evaluation of information resources of business value.[7] |
| Intercept: | Includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof.[8] |
| Internal authorization: | An authorization to intercept inmate communication that is issued by Correctional Service Canada pursuant to the *Corrections and Conditional Release Regulations*. |
| Personal call list: | A list of contacts and associated information (i.e. phone number, relationship to inmate, etc.) that an individual inmate is permitted to call.[9] |
| Transitory records: | Records that are not of business value. They may include records that serve solely as convenience copies of records held in a government institution repository, but do not include any records that are required to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to provide evidence to account for government activities.[10] |
| Warrant: | In the context of CSC's intercept activity, an authorization to intercept communication that is entered into the voice logger is called a warrant. **(REDACTED)**[11] |

[3] Inmate Telephone System, Statement of Work, November 20, 2017
[4] **(REDACTED)**
[5] https://www.csc-scc.gc.ca/acts-and-regulations/560-cd-eng.shtml
[6] **(REDACTED)**
[7] https://www.csc-scc.gc.ca/acts-and-regulations/228-cd-eng.shtml
[8] https://laws-lois.justice.gc.ca/eng/acts/c-46/
[9] Inmate Telephone System, Statement of Work, November 20, 2017
[10] https://www.csc-scc.gc.ca/acts-and-regulations/228-cd-eng.shtml
[11] **(REDACTED)**

# 1.0 INTRODUCTION

## 1.1 Background

The Audit of Interception of Inmate Communications was conducted as part of Correctional Service Canada's (CSC) 2017-2020 Risk-Based Audit Plan (RBAP). The audit links to CSC's corporate priority of ensuring the "safety and security of the public, victims, staff and offenders in institutions and in the community" [12], and to CSC's corporate risk that "CSC will not be able to maintain required levels of operational safety and security in institutions and in the community".[13]

In order to help maintain safety and security within institutions, and pursuant to requirements in the *Corrections and Conditional Release Regulations (*CCRR*)* and the *Criminal Code*, inmate communications can be intercepted to obtain intelligence information that may assist with the prevention and management of: an act that would jeopardize the security of the penitentiary or the safety of any person. CSC has been granted authority under the *Corrections and Conditional Release Act* (CCRA) to intercept inmate's private communication without receiving prior judicial authorization. Given the significance of this authority and the impact on an inmate's right to privacy, it is essential that CSC has an adequate and effective framework in place to ensure that inmate communication is intercepted in a manner consistent with legislative requirements.

**Communication Intercept**

As defined in the *Criminal Code*, the term intercept includes "listening to, recording or acquiring a communication or acquiring the substance, meaning or purport thereof." The CCRR provides CSC with the authority to intercept inmate communications including letters (mail), telephone calls, and communication during the course of a visit. In addition, CSC can be requested to intercept communication on behalf of an external agency (i.e. RCMP) pursuant to a judicial or national security authorization (authorized by a judge).

The following table shows the number of authorizations to intercept inmate communications that were issued during the 2017-2018 fiscal year.

**Table 1 - 2017-2018 Authorizations to Intercept**

| | Internal Authorizations | Judicial and National Security Authorizations | Total Authorizations to Intercept |
|---|---|---|---|
| **National** | **1062** | **3** | **1065** |

**Inmate Mail**

CSC has a responsibility to encourage inmates to maintain and develop family and community ties through written correspondence and telephone communication in a manner consistent with the principle of protection of the public, staff members and offenders.[14] Normally, the content of the mail is not to be read; however, if the inmate's communication has been authorized for interception, it will be separated during processing and provided to security intelligence staff for review, prior to being delivered.

**Inmate Telephone System[15]**

CSC has contracted Bell Canada (Bell) to provide a fully integrated inmate telephone system (ITS). **(REDACTED)**.

CSC has established individual profiles for each inmate, which is the primary data set used to manage all inmate activity on the ITS. The inmate profile includes the inmate name, unique personal identification

[12] CSC 2018-2019 Corporate Risk Profile
[13] ibid
[14] https://www.csc-scc.gc.ca/acts-and-regulations/085-cd-eng.shtml
[15] Inmate Telephone System, Statement of Work, November 20, 2017

number (PIN), finger print system (FPS) number, personal call list, applicable common call list, and current and past institution(s).

**(REDACTED)**. There are two types of call lists: common call list, and personal call list.

Common call lists contain numbers that all inmates are permitted to call. These numbers are typically associated with individuals and organizations that assist with inmate rehabilitation, some of which are privileged correspondents (i.e. Privacy Commissioner, Correctional Investigator, etc.). Users at an institution will usually determine the content of a common call list, as it applies to all inmates residing at that institution. Personal call lists contain up to a maximum of 40 phone numbers that only a specific inmate is able to call and typically include family, friends, and personal lawyers. Inmates are required to submit a written request to have a number added to their personal call list. The information provided by the inmate (i.e. name of contact, phone number, address, relationship, etc.) is required to be vetted by users for accuracy and appropriateness prior to being added to the list. Records on all call lists include mandatory information such as name of contact, phone number, relationship, and whether or not the number is allowed to be called. Call lists that an inmate is allowed to utilize are identified on the inmate profile.

Each inmate is provided with a telephone smart card (phone card) and a PIN that is linked to their inmate profile. In order to make a call, the phone card must be inserted into the payphone followed by entry of the PIN number. This provides inmates with secure access to the payphone and enables the ITS to identify the inmate. **(REDACTED)**.

**(REDACTED)**

In 2012, CSC began installing voice loggers at all institutions across the country to replace the ageing intercept equipment that was in place. **(REDACTED)**. They are owned and operated by CSC and include functionality that allows a user to record, process, and dispose of recorded communication. **(REDACTED)**.

Inmate payphones that are a part of the ITS, **(REDACTED)**.[16] **(REDACTED)**.[17]

When an inmate wants to use the payphone, they are required to provide their PIN and the phone number that they wish to call. **(REDACTED)**.[18]

**(REDACTED)**.[19]

**Communication during a Visit**

CSC has a statutory authority, when the criteria outlined in the CCRR are met, to selectively intercept and record inmate conversations. There is equipment in place in institutions that permits, when authorized, this selective interception and recording of inmate communications during the course of a visit.

**(REDACTED)**

**(REDACTED)**.

**(REDACTED)**.

**Maintenance Contracts for Communication Intercept Equipment**

A complex integrated electronic security environment has been developed and implemented in CSC's institutions across the country. The communication intercept equipment described above is a part of this environment.[20] CSC has entered into two contracts for the provision of maintenance and technical support to ensure that the communication intercept equipment functions as required. The project authority for the management of these contracts rests with the Corporate Services Sector at CSC.

**(REDACTED)**

[16] Inmate Telephone System, Statement of Work, November 20, 2017
[17] **(REDACTED)**
[18] Inmate Telephone System, Statement of Work, November 20, 201
[19] **(REDACTED)**
[20] **(REDACTED)**

**(REDACTED)**.[21] **(REDACTED)**.[22] **(REDACTED)**.

**(REDACTED)**

**(REDACTED)**.[23]

## 1.2 Legislative and Policy Framework

**Legislation**

*Canadian Charter of Rights and Freedoms*

Section 8 of the Charter provides that "everyone has the right to be secure against unreasonable search or seizure." The interception of an inmate's private communication is generally considered a search, except in circumstances where parties to the communication have given express consent to do so.

*Criminal Code*

Part 6 of the *Criminal Code* establishes the interception of an individual's private communication as an offence unless certain conditions are met. This Part outlines the authorities and legal requirements that must be adhered to in order to legally intercept an individual's private communication.

*Corrections and Conditional Release Act*

Section 96 (z.7) of the CCRA stipulates that "the Governor in Council may make regulations authorizing the institutional head – or a staff member designated by him or her – to, in the prescribed circumstances, monitor, intercept or prevent communications between an inmate and another person".

*Corrections and Conditional Release Regulations*

Sections 94 and 95 of the CCRR provides institutional heads with the authority to intercept, and stipulates the conditions that must be satisfied, in order to lawfully intercept inmate communications. It provides examples of the type of communication that may be intercepted (telephone, mail, communication during the course of a visit); the means by which the communication can be intercepted (i.e., use of mechanical device, reading of mail, etc.); and the requirements for notifying the inmate that their communication has been intercepted.

*Privacy Act*

The purpose of this Act is to "extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."[24] Sections 4-7 outline the requirements for the collection, retention, protection, disclosure, and disposal of personal information.

**CSC Policy Instruments**

There are a number of Commissioner's Directives (CDs), Guidelines (GL) and Institutional Standing Orders which provide guidance for, or relate to, the interception of inmate communications (refer to Annex D for a complete list). The following CDs provide the majority of that guidance.

CD 568 Management of Security Information and Intelligence

The purpose of this CD is "to ensure consistency in the collection, storage, collation, recording, reporting and disposal of security information and intelligence, and to ensure a consistent approach for the communication and sharing of security information and intelligence to individuals who have an identified need to know."[25] It sets out roles and responsibilities for the management of the security intelligence function, and defines the procedures for the management of security intelligence and information.

[21] ibid
[22] **(REDACTED)**
[23] **(REDACTED)**
[24] Privacy Act - https://laws-lois.justice.gc.ca/eng/acts/P-21/
[25] https://www.csc-scc.gc.ca/acts-and-regulations/568-cd-eng.shtml

CD 568-2 Recording and Sharing of Security Information and Intelligence

The purpose of this CD is "to ensure timely recording and sharing of security information and intelligence to promote dynamic security."[26] It outlines roles and responsibilities of management and staff, as well as the procedures for the collection, documentation, evaluation, and reporting of information.

CD 568-10 Interception of Inmate Communications

The purpose of this CD is "to provide direction to staff and define the prescribed circumstances under which the lawful interception of communications between an inmate and another person may be requested, authorized and conducted."[27] It sets out roles and responsibilities for management and staff, outlines the parameters for designating authority to authorize, and the rules that must be followed to intercept inmate communications.

Institutional Standing Orders (SO)

In accordance with CD 568-10, the "institutional head will ensure that a standing order is in place detailing the procedures for interception of inmate communications." The SO also serves as the mechanism by which the institutional head may designate authority to: authorize the interception of inmate communications, and notify the inmate of the interception.

## 1.3 CSC Organization

**National Headquarters (NHQ)**

The Assistant Commissioner, Correctional Operations and Programs (ACCOP) is responsible for developing policies for the security intelligence function.[28]

The Director General, Preventive Security and Intelligence (PSI) is responsible for implementing a framework for security intelligence and analysis and developing the policy and procedures related to the interception of inmate communications.

The Director General, Technical Services and Facilities is responsible for: the design and management of contracts for the acquisition, installation, or repair or any systems or devices utilized in the interception process; ensuring that contractors and suppliers are licensed in accordance with the *Criminal Code*; and developing the maintenance standards for all interception-related equipment in the institutions.[29]

**Regional Headquarters (RHQ)**

The Regional Deputy Commissioner (RDC) is responsible for ensuring that the intelligence operations and analysis are supported at the regional level.

The Assistant Deputy Commissioner, Correctional Operations (ADCCO) is responsible for: the planning and provision of direction on security operations and intelligence activities for the region; ensuring that policies are effectively communicated to operational units; overseeing the implementation of operational protocols, policies and administrative controls to ensure consistent application of security information and intelligence procedures; and ensuring that operational reviews of policies are conducted on a regular basis and that any issues arising from policies, procedures or their implementation are reported in a timely manner to NHQ.[30]

**Institutions**

The Institutional Head (IH) is designated the authority to intercept inmate communications through the CCRR. Further, the IH is responsible for ensuring: that there is an effective intelligence function at each operational site[31]; a standing order is in place that outlines the procedures for interception of inmate

[26] https://www.csc-scc.gc.ca/acts-and-regulations/568-2-cd-eng.shtml
[27] https://www.csc-scc.gc.ca/acts-and-regulations/568-10-cd-eng.shtml
[28] https://www.csc-scc.gc.ca/acts-and-regulations/568-cd-eng.shtml
[29] https://www.csc-scc.gc.ca/acts-and-regulations/568-10-cd-eng.shtml
[30] https://www.csc-scc.gc.ca/acts-and-regulations/568-cd-eng.shtml
[31] ibid

communications; and authorizing and/or designating authority to authorize the interception of inmate communications.[32]

The Deputy Warden (DW) is responsible for security intelligence in an institution and approving the interception of inmate communications.[33]

The Security Intelligence Officer (SIO) is responsible for the collection and analysis of information from all sources and the development of intelligence to enhance public safety.[34] Generally speaking, they are responsible for all interception of inmate communication activities, including but not limited to: gathering and providing details for requesting authorization to intercept, conducting the intercept, documenting and reporting intercept activities, preparing intelligence reports, and sharing intelligence information with internal and external stakeholders.[35]

## 1.4 Risk Assessment

In February 2018, following consultations with senior management at NHQ, interception of inmate communications was identified as an area of emerging risk. An engagement level risk assessment was completed by the audit team using the results of interviews and documentation review to determine areas of intercept activity that the audit should cover. Overall, the assessment identified key risks associated with the management framework in place as well as the implementation of key controls. These risks were incorporated into this audit to assess whether mitigation strategies are sufficient.

[32] https://www.csc-scc.gc.ca/acts-and-regulations/568-10-cd-eng.shtml
[33] https://www.csc-scc.gc.ca/acts-and-regulations/005-1-gl-eng.shtml
[34] https://www.csc-scc.gc.ca/acts-and-regulations/568-cd-eng.shtml
[35] https://www.csc-scc.gc.ca/acts-and-regulations/568-10-cd-eng.shtml

# 2.0 OBJECTIVES AND SCOPE

## 2.1 Audit Objectives

The objectives of this audit were to provide assurance that:

- The management framework in place supports the efficient and effective achievement of communication intercept objectives; and
- Key activities have been implemented in compliance with requirements.

Specific criteria are included in Annex B.

## 2.2 Audit Scope

### 2.2.1 Phase 1

Phase 1 of the audit was national in scope and included visits to three regions and NHQ. File review focused on a sample of communication intercepts that were approved and completed from January 1, 2017 – June 22, 2018. The sample covered communication intercept activity that was approved internally as well as those that were carried out pursuant to either a judicial security or national security authorization (approval given by a judge).

Phase 1 included an analysis of three methods of intercepting communication: telephone; communication during the course of a visit; and mail; however, testing for mail and V&C communication intercept activity was limited to observations and interviews with staff.

Phase 1 was planned to include visits to institutions in all five regions; however, after completing audit work in the third region, sufficient evidence had been obtained to conclude against objectives. Therefore, the audit did not include visits to either the Quebec or Atlantic regions.

### 2.2.2 Subsequent Events

The audit team provided briefings to senior management at NHQ and in the three regions immediately upon completion of its site visits. In response, the Senior Deputy Commissioner in collaboration with ACCOP and the RDCs prepared an action plan to immediately address the most significant preliminary findings from the audit. The actions taken by management focused on the following three areas: providing updated guidance to institutions; providing training to institutional management and SIOs on the legal and policy framework as well as on the voice logger; and implementing oversight and quality assurance processes at both RHQ and NHQ over authorizations to intercept.

### 2.2.3 Phase 2

Phase 2 assessed if management actions were effective in addressing the most significant issues raised through Phase 1 of the audit. The specific audit criteria that were re-examined through Phase 2 are included in Annex B.

Phase 2 was national in scope and included visits to all five regions. File review focused on a sample of communication intercepts that were approved and completed from November 1, 2018 – April 12, 2019. The sample did not re-examine communication intercept activity that was approved externally, mail interception, or communication during the course of a visit.

# 3.0 AUDIT FINDINGS AND RECOMMENDATIONS

## 3.1 Management Framework – Phase 1 Results

The first objective for this audit was to provide assurance that the management framework in place supports the efficient and effective achievement of communication intercept objectives.

The management framework was examined from four perspectives: CSC's guidance; training; communication intercept equipment; and monitoring. Annex B provides general results for all audit criteria.

### 3.1.1 Guidance

We expected to find that CSC guidance was complete, clear, and aligned with legislation.

The following areas met the audit expectations for this criterion:

- CD 568-10 Interception of Inmate Communications aligned with the CCRR; and
- 11/11 institutions we visited had a standing order in place.

As described below, there were two areas related to guidance that warranted further consideration by management.

***Direction provided in CDs was unclear and incomplete.***

CD 568 Management of Security Information and Intelligence, CD 568-2 Recording and Sharing of Security Information and Intelligence, and CD 568-10 Interception of Inmate Communications are the primary policy instruments in place that establish the rules that are to be followed for the interception of inmate communications, and assign roles and responsibilities. These CDs were all due for review in November 2015; however, this review had yet to occur at the time of the audit. In addition, we found that these CDs did not provide clear and complete direction for the following areas:

- The definition of the term intercept, as provided in the *Criminal Code*, was not included in national guidance;
- Reasonable grounds to believe was not defined in national guidance (refer to 3.2.1 for more information);
- National guidance did not indicate that approval must be provided in writing prior to intercepting communication as required by the CCRR (refer to 3.2.2 for more information);
- The roles and responsibilities of V&C staff in the intercept process was not included in national guidance (refer to 3.2.3 for more information);
- National guidance for documenting ITS intercepts did not incorporate the automated audit trails available in the voice logger (refer to 3.2.3 for more information);
- The retention period for intercepted communication was not included in national guidance (refer to 3.2.4 for more information);
- The recorded communication that should be archived onto DVD was not clearly articulated in national guidance (refer to 3.2.4 for more information); and
- The manner in which inmates were to be notified that their communication had been intercepted was not included in national guidance (refer to 3.2.4 for more information).

While there were a variety of specific causes for the issues identified above, which are further explored in the following sections, effective monitoring and oversight practices would have provided valuable information that could have shed light on these issues and served as a catalyst for evaluating and updating guidance.

***Institutional standing orders did not always align with CSC's national guidance and the CCRR.***

CD 568-10 requires the IH to ensure that "a standing order is in place detailing the procedures for interception of inmate communications". We completed a review of SOs to ensure that the institutional procedures were documented and aligned with the CCRR and national guidance. We found that the direction provided in SOs was generally a copy and paste of that in CD 568-10 and provided little to no additional guidance around the procedures that should be utilized when intercepting communication. Further, we identified the following issues in the SOs that we reviewed:

- 1/11 included direction for inmate notification that was non-compliant with the CCRR;
- 3/11 allowed for intercept activity to be carried out in emergency situations without approval in place, which was non-compliant with the CCRR;
- 3/11 included designation of authority to approve the interception of inmate communications to positions other than DW, which was non-compliant with CD 568-10;
- 3/11 included direction where V&C staff can seek authorization to intercept communication in emergency situations, which was non-compliant with CD 568-10;
- 4/11 included an incomplete list of privileged communication, which could lead to non-compliance with the CCRR; and
- 2/11 included references to CDs that were no longer in place.

Interviews with management from PSI revealed that the expectation of the extent of information that should be included in SOs in order to comply with national guidance had not been clearly defined. In addition, SOs had not been adequately developed and reviewed to ensure that the guidance provided was compliant with CD 568-10 and the CCRR.

Overall, the CDs and SOs did not provide clear and complete guidance for the interception of communication. This has led to operational inefficiencies and has ultimately contributed to the interception of communication in a manner that was non-compliant with legislative requirements.

### 3.1.2 Training

We expected to find that CSC provided training to support the discharge of responsibilities.

The following areas met the audit expectations for this criterion:

- National training standard (NTS) and non-NTS training was developed and provided to SIOs;
- NTS training that included information on the standard of proof (reasonable grounds to believe) that must be met in order to legally intercept communication had been developed and provided to institutional management; and
- The completion of training was being monitored.

As described below, there were two areas related to training that required further consideration by management.

***Training on the legal and policy framework was not sufficient.***

We reviewed the NTS and found that there has been an SIO orientation course in place for many years; however, this course was offered one-time only and was to be completed within 12 months of becoming an SIO. While completion rates for this training was 90% as of September 2018, 38% of the SIOs completed the training prior to 2010, at which time the course did not cover communication intercepts.

We should acknowledge that SIOs were provided with non-NTS training in winter 2018. This training included information on reasonable grounds to believe, but did not include any other information on the legal and policy framework for communication intercepts.

Recently, a continuous development training for SIOs was added to the NTS, with delivery of this training beginning in the fall of 2018.

In addition, IHs and DWs (decision makers) felt that the training they receive could be improved. The only NTS for decision makers that included training on the interception of communication was the Operational Senior Manager Training Program. While this course included information on reasonable grounds to believe, it did not include any other information on the legal and policy framework. This course was offered one-time only with no refresher training and was only required for DWs. Completion rates for DWs was 69% as of September 2018. Management within the Learning and Development Branch at NHQ indicated that resourcing pressures and limited course offerings made it difficult at times for DWs to receive the NTS training within the required timeframes.

Insufficient training for both decision makers and SIOs contributed to a lack of understanding of key legal and policy requirements in place. Specifically, we found that:

- Decision makers and SIOs did not have a good understanding of 'reasonable grounds to believe', including how it should be documented (refer to 3.2.1 for more information);
- Decision makers and SIOs did not understand that approval must be given in writing prior to intercepting communication (refer to 3.2.2 for more information);
- SIOs did not understand what information should be archived onto DVD (refer to 3.2.4 for more information); and
- Decision makers and SIOs did not understand requirements for notifying inmates that their communication had been intercepted (refer to 3.2.4 for more information).

This has ultimately contributed to the interception of inmate communications in a manner that was non-compliant with legislative requirements.

***Training on the voice logger was available; however, it had not been provided.***

CSC has a contract in place with **(REDACTED)**, which includes a provision for training on the voice logger. While responsibility for managing this contract rests with the Corporate Services Sector (CSS) at NHQ, roles and responsibilities for ensuring that SIOs receive training on the voice logger had not been defined. We found that a copy of the contract had not been shared by CSS and as a result institutional management and SIOs were not aware that training was available on the voice logger. In addition, user manuals were in place that provided direction on the functionality and use of the voice logger. Results of our interviews revealed that SIOs had never received formal training on the voice logger, and while they were aware that manuals are in place, they had not reviewed them to learn how to properly use the system.

The lack of training and use of the user manuals led to SIOs having very limited knowledge of the functionality and operation of the voice logger. This resulted in significant non-compliance with the CCRR, most notably the interception of privileged communications (refer to section 3.2.3 for more information).

### 3.1.3 Equipment

We expected to find that CSC had the necessary equipment in place to intercept inmate communications.

The following areas met the audit expectations for this criterion:

- Voice loggers were in place at all institutions and enabled staff to effectively intercept inmate communications; and
- SIOs indicated that they were generally satisfied with the services they received from **(REDACTED)** technicians.

As described below, there was one area related to equipment that required further consideration by management.

**(REDACTED).**

**(REDACTED)**.

**(REDACTED)**.

### 3.1.4 Monitoring

We expected to find that monitoring was conducted on a regular basis and results were documented and reported to the required management level.

As described below, there was one area related to monitoring that required further consideration by management.

***Monitoring and reporting mechanisms were insufficient at the local, regional, and national levels.***

Management at all levels had not established key performance indicators that could be used to guide monitoring and reporting activities (i.e. information to collect, including frequency and format, etc.). While CD 568-10 required that SIOs "report intercepted activities to the director, Intelligence Operations, Policy and Programs, via the ADCCO"; management at RHQ and NHQ had not established what information should be reported. **(REDACTED)**. As a result, we found that no monitoring information was reported to any level, which limited management's ability to provide effective oversight of the interception of communication.

"The Compliance and Operational Risk Report (CORR) is an internal management tool used to monitor implementation and quality of internal policies, and to establish a risk-aware culture within CSC".[36] It utilizes a self-assessment questionnaire that is comprised of a series of criteria and sub-questions that are designed to determine compliance for a specific activity. Communication intercepts was included in the CORR that was completed in the fall of 2017 and was the only monitoring mechanism in place at NHQ upon completion of Phase 1 of the audit. The criteria selected for the CORR assessment did not include a number of key legal requirements such as approvals to intercept, inmate notifications, and designation of authority. While analysis was completed of the results and corrective action identified for noted deficiencies, the actions taken were not effective as we found the same issues during our audit testing. Further, we found that rationale provided by sites for non-compliance did not lead to an analysis of the direction provided in CDs. For example, institutions consistently indicated that they do not utilize CSC form 1036 *Record of Intercepted Communications* to document intercept activity, **(REDACTED)**. However, this did not trigger a review of requirements around documenting intercept activity, which could have highlighted that the functionality of the voice logger was not reflected in national guidance.

The lack of monitoring and reporting limited CSC's ability to manage the interception of inmate communications effectively. The limited monitoring in place did not provide management with the required information to be able to assess the appropriateness of guidance, adequacy of resourcing, compliance with legal requirements, and whether or not objectives were being achieved efficiently and effectively.

### Conclusion – Objective 1

Through Phase 1 of this audit, we found that elements of a management framework were in place; however, improvements were required to help ensure that the framework supports the efficient and effective achievement of communication intercept objectives. Specifically, a lack of guidance and limited training caused institutional management and SIOs to have an incomplete understanding of the legal and policy requirements for intercepting inmate communications, which resulted in significant compliance issues. These compliance issues, which are described in the second objective of this audit report, have gone largely undetected due to insufficient quality assurance over the intercept work performed by the SIOs, and a lack of monitoring and reporting activity.

## 3.2 Communication Intercept Activity – Phase 1 and 2 Results

The second objective for this audit was to provide assurance that key activities supporting the interception of inmate communications have been implemented in compliance with requirements.

Compliance was assessed from four perspectives: reasonable grounds, approval to intercept, compliance with approvals, and information security and sharing. Annex B provides general results for all audit criteria.

[36] CORR Application information available on CSC's intranet

### 3.2.1 Reasonable Grounds

We expected to find that reasonable grounds were adequately documented and supported by intelligence information.

As described below, there were two areas related to reasonable grounds that required further consideration by management.

***Reasonable grounds were not always adequately documented.***

Pursuant to section 94. (1) of the CCRR "the institutional head or a staff member designated by the institutional head may authorize, in writing, that communications between an inmate and a member of the public, including letters, telephone conversations and communications in the course of a visit, be opened, read, listened to or otherwise intercepted by a staff member or a mechanical device, where the institutional head or staff member believes on reasonable grounds

(a) that the communications contain or will contain evidence of

(i) an act that would jeopardize the security of the penitentiary or the safety of any person, or

(ii) a criminal offence or a plan to commit a criminal offence; and

(b) that interception of the communications is the least restrictive measure available in the circumstances".[37]

CD 568-10 requires that CSC form 1454 Authorization to Intercept Inmate Communications (approval form), be completed in its entirety and maintained on file by an SIO. This form includes a section for documenting a gist of the information being relied upon to establish the reasonable grounds.

We reviewed a sample of files to determine if reasonable grounds were documented, and if the information provided was adequate to persuade an independent third party to believe that the conditions stated in the CCRR (i.e. communications contain or will contain evidence of) have been met. We found that reasonable grounds were documented in 96% (80/83) of the files reviewed. For the three files where the grounds were not documented, SIOs indicated that the approval form had been completed, but they were unable to locate it. Further, we found that reasonable grounds were adequately documented for 60% (48/80) of the files. In general, the extent of information documented to establish reasonable grounds varied significantly from one file to another, typically did not reference supporting information, and at times was limited to one or two sentences (i.e. inmate found unresponsive in cell).

The reasonable grounds were prepared by an SIO and provided to the decision maker for review and approval. SIOs indicated that they felt that the extent of information that should be documented to demonstrate reasonable grounds was subjective, was not clearly articulated in CSC guidance, and varied depending on the decision maker. Decision makers indicated that while they felt they understood what should be documented, this was based on their experience as they had never been challenged on the adequacy of their documentation, nor had they been provided with examples of properly documented reasonable grounds. We found that the guidance provided in CD 568-10 did not further define or provide clarification as to how reasonable grounds should be documented. In addition, we found that there was no challenge function or review of the information provided on approval forms from RHQ/NHQ.

The lack of clear guidance and oversight combined with the limited training decision makers and SIOs have received resulted in a lack of adequately documented reasonable grounds. This in turn limited CSCs ability to demonstrate the information that was taken into consideration by the decision maker to ensure that the standard of proof required by the CCRR to justify the interception of communication had been met.

**Information establishing reasonable grounds was often not clearly referenced and documented.**

*Mugesera* v. *Canada (Minister of Citizenship and Immigration), [2005]*[38]*,* outlines that "reasonable grounds will exist where there is an objective basis for the belief which is based on compelling and credible information". As required by CD 568-10, SIOs are responsible for gathering and providing details or evidence for requesting authorization to lawfully intercept an inmate's communication. The information

[37] https://laws.justice.gc.ca/eng/regulations/SOR-92-620/page-8.html#h-48
[38] https://www.canlii.org/en/ca/scc/doc/2005/2005scc40/2005scc40.html?resultIndex=1

gathered is documented and maintained in the inmate's preventive security file. A gist of this information is then documented on the approval form to demonstrate that there is reasonable grounds to intercept an inmate's communication.

We reviewed a sample of files to determine if the reasonable grounds clearly referenced the supporting intelligence information, and that the information being referenced existed (documented in the preventive security file). We found that supporting information was clearly referenced for only 38% (30/80) of the files reviewed. Of these 30 files, the information being referenced was documented for 93% (28/30).

SIOs indicated that they did not always have enough time to ensure that information being relied upon to establish reasonable grounds was documented as required prior to seeking approval to intercept due to a lack of human resources. Further, approval processes in place did not include a review of the supporting information to ensure that it was documented.

The lack of clear referencing to supporting documentation limited CSC's ability to demonstrate that the information being relied upon to establish reasonable grounds was compelling, credible, and existed.

**Phase 2 Results**

Upon completion of Phase 1 in Autumn 2018, CSC provided training to IHs and DWs that included guidance on what constitutes reasonable grounds. Participants were provided with reference material that included examples of adequately documented reasonable grounds. These actions were put in place to address deficiencies noted during Phase 1.

Results of the file review for Phase 2 revealed that:

- Reasonable grounds were documented: 100% (62/62)
- Reasonable grounds were adequately documented: 79% (49/62)
- Reasonable grounds clearly referenced the supporting intelligence information: 81% (50/62)
- The intelligence information being referenced was documented: 86% (36/42)

**(REDACTED)**.

Overall, results from Phase 2 for reasonable grounds demonstrate improvement. However, continued management attention will help ensure that reasonable grounds are adequately documented to demonstrate compliance with the CCRR, and the supporting intelligence information is compelling, credible, and exists.

### 3.2.2 Approval to Intercept

We expected to find that approval to intercept was given in writing, by an individual with the appropriate authority, prior to the start of related intercept activity.

As described below, there were two areas related to approval to intercept that required further consideration by management.

***Approval to intercept was not always given in writing, by an individual with appropriate authority, prior to the start of the authorized intercept period.***

Pursuant to section 94. (1) of the CCRR "the institutional head or a staff member designated by the institutional head may authorize, in writing, that communication between an inmate and a member of the public"[39] be intercepted. CD 568-10 further requires that these approvals are provided in writing on the approval form.

We reviewed a sample of files and found that approval was provided in writing by an individual with appropriate authority for 96% (80/83) of the files reviewed. Further, we found that the written approval was

[39] https://laws.justice.gc.ca/eng/regulations/SOR-92-620/page-8.html#h-48

provided prior to the start of the authorized intercept period for 93% (77/83) of the files reviewed. The following is a breakdown of the issues noted:

- Approval forms were not on file for 4% (3/83) of the files reviewed (no written approval);
- Authorization date was not documented on the approval form for 2% (2/83) of the files reviewed; and
- Verbal approval was provided for 1% (1/83) of the files reviewed, with written approval provided four days later.

Although we only found evidence of verbal approval in one of the files reviewed, interviews revealed that decision makers at 9/11 institutions would provide verbal approval when they believed it was necessary (i.e. decision maker not on site, perceived need to intercept communication as soon as possible to gather timely and pertinent information) and completed the approval form afterwards. This practice was non-compliant with the CCRR. In addition, we were informed at 2/9 sites that they would backdate the written approval to reflect the date that verbal approval was given. It should be noted that this practice may have improved the results of our file review.

A review of CD 568-10 revealed that the requirements around authorization did not clearly state that approval must be given in writing prior to the start of the authorized intercept period. The lack of clear guidance combined with the limited training that decision makers and SIOs had received resulted in a lack of understanding of the legal requirement around approval to intercept, which increased the risk of intercepting communication prior to written approval. In addition, the situations where we found that an inmate's communication was intercepted without written approval in place was non-compliant with the CCRR.

**Phase 2 Results**

Upon completion of Phase 1 in autumn 2018, CSC provided training to IHs and DWs that included guidance on legislative requirements for approving the interception of communications and the manner in which these approvals are to be given.

Results of the file review for Phase 2 revealed that:

- Approval was provided in writing: 98% (61/62)
- Approval was provided prior to the start of the authorized intercept period: 94% (58/62)

While improvements have been made, the persistence of these issues further demonstrate the need to implement quality assurance processes to ensure compliance with the CCRR.

***Intercepts were often approved for timeframes that exceeded those provided for in CD 568-10.***

As per CD 568-10, "the initial interception can only be authorized for a maximum period of 30 days. If required, the interception can be extended for up to two additional periods of 15 days. All extensions must be authorized by the Institutional Head or Deputy Warden, prior to the expiry of the existing authorization".

Through our file review we found that approvals were provided for a period of less than or equal to 30 days in only 41% (32/79) of the files reviewed. In addition, of the 28 extensions reviewed, 57% (16/28) were approved for a period of less than or equal to 15 days.

This was primarily caused by the SIO documenting the end date as one month (i.e. Jan.5 – Feb.5) after the start date on the approval form, which in some cases equated to 31 days. The high rate of non-compliance demonstrated a lack of quality control of the approval form prior to authorization by a decision maker.

**Phase 2 Results**

Results of the file review for Phase 2 revealed that:

- Initial intercepts were approved for a period of less than or equal to 30 days as required by CD 568-10: 82% (51/62)
- Extensions were approved for a period of less than or equal to 15 days as required by CD 568-10: 79% (11/14)

While significant improvements have been made, the persistence of these issues further demonstrate the need to implement quality assurance processes to ensure compliance with CD 568-10.

### 3.2.3 Compliance with Approval

We expected to find that communication intercepts were carried out in compliance with approvals.

The following area met the audit expectations for this criterion:

- SIOs and V&C staff indicated that clear and effective processes were in place for intercepting inmate's mail at 11/11 institutions we visited.*

As described below, there were four areas related to compliance with approval that required further consideration by management.

***Telephone calls were intercepted outside of the authorized time period.***

We reviewed a sample of files and found that communication was intercepted within the authorized time period for 88% (68/77) of the files reviewed. Of the nine non-compliant files, we found 256 phone calls that were intercepted after the authorized period had expired and many of these calls were accessed by SIOs.

There were two main issues that led to the non-compliant activity. First, we found that SIOs did not always seek written approval for extensions prior to the expiry of the authorization in place due to a lack of formal processes to track intercept time periods. This led to situations where there were gaps in the authorized time periods for which SIOs did not accurately amend the warrants in the voice loggers; ultimately resulting in inmate's phone calls being recorded without written authorization in place. Second, we found data entry errors with the intercept time periods entered into the voice logger. We noted that when warrants were entered into the voice logger, there was no quality assurance of the information that was entered to ensure it was accurate. As a result, data entry errors have gone undetected and inmate's communication have been intercepted without authorization in place, which was non-compliant with the CCRR.

**Phase 2 Results**

Upon completion of Phase 1 in Autumn 2018, CSC provided training to the SIOs on the voice logger. The training included guidance on how to create a warrant as well as the importance of accurately entering the warrant information.

We found that communications were intercepted within the authorized time period for 97% (60/62) of the files reviewed. Of the extensions we reviewed, 93% (13/14) were signed prior to the expiry of the authorization, which contributed to the improved compliance rate for Phase 2.

While progress has been made, the persistence of these issues further demonstrate the need to implement quality assurance processes to ensure compliance with the CCRR.

* The audit team was unable to confirm the effectiveness of mail intercept activity due to a lack of audit trail.

***Unauthorized interception by Visits and Correspondence staff.***

As outlined in the background, **(REDACTED)**. As per CD 568-10, "access to devices utilized in the interception of inmate communications should be restricted to authorized individuals whose duties require access on a need to know basis".

During interviews, decision makers, SIOs, and V&C staff themselves indicated that they were aware of situations where V&C staff have used the equipment without approval to do so. **(REDACTED)** without prior written approval or any record of this activity, which significantly increased the risk of unauthorized and inappropriate use.

***Privileged communication was intercepted without approval.***

Pursuant to section 94. (2) of the CCRR, "No institutional head or staff member designated by the institutional head shall authorize the opening of, reading of, listening to or otherwise intercepting of communications between an inmate and a person set out in the schedule by a staff member or a mechanical device, unless the institutional head or staff member believes on reasonable grounds:

(a) that the grounds referred to in subsection (1) exist; and

(b) that the communications are not or will not be the subject of a privilege."

Refer to Annex E for a list of individuals considered privileged communication.

Through file review we found that communication between an inmate and their lawyer was intercepted without approval for 10% (8/79) of the files reviewed, resulting in a potential breach of solicitor-client privilege. In total, 25 phone calls were recorded and four of them were accessed. For six of these files, we found that SIOs did not add the lawyer's phone number(s) to the **(REDACTED)** when creating the warrant. Effective quality assurance over the information entered into the voice logger would have caught these omissions; however, we found that these safeguards were not in place. For the remaining two files, we found that V&C staff added lawyers' phone numbers to the inmate's 'personal call list' while there was an active warrant for that inmate in the voice logger. The addition of the lawyer's phone number was not communicated to an SIO and as a result, they were not aware of the need to update the **(REDACTED)**.

**(REDACTED)**. We completed an analysis of the **(REDACTED)** to determine if all of the contacts in the common call list that represent privileged communication were included. We found that none of the **(REDACTED)** we visited. While we did not assess whether or not phone calls to these privileged correspondents had been recorded, **(REDACTED)**. SIOs at all institutions we visited indicated that they were not aware of the **(REDACTED)** and as a result were not aware of the need to maintain them **(REDACTED)**. The interception of privileged communication without approval to do so was non-compliant with the CCRR.

**Phase 2 Results**

Upon completion of Phase 1 in Autumn 2018, CSC provided training to the SIOs on the voice logger. The training included guidance for how to **(REDACTED)**. In addition, PSI issued a Security Bulletin in September 2018 that reminded SIOs to suppress all privileged communication and required institutions to implement a process where any new phone number associated with privileged communication is shared with an SIO prior to being entered in the ITS.

Results of our document and file review for Phase 2 revealed that:

- Communications between an inmate and their lawyer was suppressed: 95% (59/62)
- A process was in place at the sites we visited to share privileged phone numbers with an SIO prior to the number being entered in the ITS: 0% (0/12)
- **(REDACTED)** were up-to-date at the sites we visited: 18% (2/11)

While the results from Phase 2 represent a slight improvement, it again highlights the need to implement quality assurance processes so that information entered into the voice logger is complete, accurate, and up-to-date, to ensure that communication is intercepted in compliance with the CCRR.

***Intercept activity was not documented as required.***

As per CD 568-10, SIOs are required to "maintain a record of all interception activity and the disposition of the information gathered through interception" using CSC form 1036 Record of Intercepted Communications (form 1036). These logs provide a means of ensuring that the integrity of the information collected is maintained, which is essential if it is to be used as evidence in any form of administrative or judicial procedure. Further, it provides a basis for tracking personal information that is collected, to help ensure that it is used, maintained, and disposed of in accordance with the *Privacy Act*.

Through file review we found that recorded telephone calls were documented on form 1036 for 25% (20/79) of the files reviewed. Further, we found that the disposition (i.e. information is useful or not) of information obtained through ITS communication intercepts was documented on form 1036 for only 13% (10/79) of the files reviewed. SIOs indicated that they did not complete form 1036 as the voice logger includes an automated log of all intercept activity, which included the information required to be completed on CSC form 1036, with the exception of: the name of the person called, if the intercepted communication was summarized or not, and the disposition of the information. **(REDACTED)**. However, we found that this functionality was not incorporated into CSC guidance and SIOs had not received training on the voice logger. As a result the documentation of ITS intercept activity was typically incomplete. In our view, the requirement to manually document intercepted telephone calls using form 1036 is a redundant task that creates inefficiency in the process.

Interviews with SIOs at 10/11 of the institutions we visited, revealed that they did not utilize form 1036 to track mail and V&C intercepts, therefore there was no record of this activity at all. The lack of documentation of mail and V&C intercept activity resulted in the interception of communication without any record of it occurring, including the name of the individual that completed the intercept, which could impact the ability to use the information as evidence. Further, it impedes management's ability to monitor intercept activity and could limit CSC's ability to ensure that personal information that is collected is used, maintained, and disposed of in accordance with the *Privacy Act*.

### 3.2.4 Information Security and Sharing

We expected to find that information was appropriately secured and shared.

The following areas met the audit expectations for this criterion:

- Voice loggers were maintained in secure locations within institutions and physical access was well controlled;
- Business level processes were in place to control access to preventive security files; and
- SIOs indicated that intelligence information obtained through communication intercepts was often used to help maintain the safety and security of institutions.

As described below, there were four areas related to information security and sharing that required further consideration by management.

***User accounts in the voice logger were not properly used or maintained.***

Pursuant to CD 225 Information Technology Security, all authorized users of CSC's IT systems will be uniquely identified in the system so that access to sensitive information can be both controlled and monitored. Authorizations are to be granted on a need-to-know basis and limited to minimum access required for the individual to perform his/her duties. We completed an analysis of user accounts on the voice logger and found:

- 18/22 SIOs had their own user accounts at the nine sites we assessed;
- **(REDACTED)** at 9/9 sites;
- All user accounts, including those for **(REDACTED)** technicians, were assigned administrative access; and
- SIOs at 6/11 sites indicated that they would often share user accounts.

We found that standards for the maintenance of user accounts and appropriate levels of access to the voice logger had not been defined, nor had responsibility for maintaining user accounts. As a result, all user accounts were assigned administrative privileges by default, which enabled the user to **(REDACTED)**. Further, we found that user accounts were not deleted when the user no longer had an identified need to know.

The lack of proper control and use of user accounts increased the following risks: **(REDACTED)**. In addition, these issues increased the risk of non-compliance with central agency policies and the *Privacy Act* around information security, and **(REDACTED)**.

***Transitory information was not disposed of in accordance with information life cycle requirements.***

As per CD 228 Information Management "to ensure government privacy and security requirements around information are met, transitory information is to be regularly disposed of after it is no longer required." **(REDACTED)**.

Our file review revealed that a vast majority of the recordings on the voice loggers were actually transitory, with no identified business value. We found that CSC had not defined retention periods for information obtained through communication intercepts and the **(REDACTED)**. In addition, SIOs at 9/11 institutions indicated that they archived all audio recordings (including transitory) onto DVD and maintained these in perpetuity. As a result, every audio recording since the voice loggers were first put in place in 2012, were likely still maintained on the hard drives, and in most cases in duplicate on DVD as well.

The lack of information management practices resulted in non-compliance with the *Privacy Act*. This issue was exacerbated by the fact that some of these recordings were that of privileged communication (refer to section 3.2.3 for more information).

***Sharing of intelligence information was not always documented.***

CD 568-2 requires SIOs to complete *CSC form 1443 Security Intelligence Briefing Record* to record the various security intelligence briefings that are presented to management, staff members, or members of outside agencies. SIOs indicated that they shared intelligence information with internal and external stakeholders on a regular basis, both verbally and in writing (i.e. IOR/SIR). While the verbal sharing of information constituted a security intelligence briefing, SIOs at all institutions visited indicated that they did not utilize form 1443 to document the information that was shared due to a lack of time and resources. It should be noted that CD 568-2 is currently undergoing revision and the requirements for documenting security intelligence briefings are being amended.

The lack of documentation impeded CSC's ability to track the sharing of personal information and limited management's ability to monitor information sharing to ensure compliance with the *Privacy* Act.

***Inmates were not always notified of intercept activity.***

Pursuant to section 94. (3) of the CCRR "where a communication is intercepted under subsection (1) or (2), the institutional head or staff member designated by the institutional head shall promptly inform the inmate, in writing, of the reasons for the interception". CD 568-10 further requires that SIOs use CSC form 1135 Notice of Interception of Communications (notification form) to inform the inmate of the reasons for the interception, which is to be given to the inmate either promptly upon completion of the interception, or upon completion of the associated investigation if the notification is deemed to have an adverse affect on that investigation.

The notification form does not include a section for the inmate to sign to attest to the fact that they have received it, nor does it include a section for a witness signature in cases where the inmate refuses to sign. So while we found completed notification forms on file for 88% (68/77) of the files reviewed, there was no evidence on any of them that it had been provided to the inmate. In addition, SIOs indicated that they signed and dated the notification forms the day that they prepared them and not on the day that it was provided to the inmate. This left CSC in a position where it was not able to demonstrate if and when inmates were actually notified.

We also found issues with the processes in place to share the notification form with the inmate. SIOs at all institutions we visited indicated that they typically mailed the completed notification form to the inmate, which did not ensure that the form was actually received by the inmate. In addition, one site would put the

notification form on the inmate's admission and discharge file, which the inmate would only be able to access upon release/transfer from the institution. This could result in situations where the inmate was not notified for a significant period of time, and potentially never if they were not released from the institution.

Interviews with management in the Preventive Security and Intelligence Branch indicated that their general expectation was that SIOs should provide the notification forms to inmates in person, as this guaranteed the inmate received the form, provided the inmate with an opportunity to make representations, and could lead to SIOs obtaining additional intelligence. This expectation was not articulated in CSC guidance.

The design flaws, such as no inmate or witness signature block, with the notification form limited CSCs ability to demonstrate that inmates were actually notified as required by the CCRR. Further, the lack of clear guidance resulted in inconsistent and inappropriate business level processes for inmate notification, which increased the risk of non-compliance with the CCRR.

## Conclusion – Objective 2

We found that several of the key activities associated with the communication intercept process were not always compliant with requirements. Specifically, reasonable grounds were often not adequately documented and/or supported by intelligence information, authorization to intercept an inmate's communication was not always provided in writing, and communication (including that which is privileged) was intercepted without approval. We also identified that intercept activity was not always well-documented, and information obtained through intercept activity was not always properly managed. In addition, we found a lack of effective safeguards to ensure that CSC was meeting its legal and policy obligations with respect to notifying inmates that their communication had been intercepted.

### Recommendation 1

The Assistant Commissioner, Correctional Operations and Programs should revise national guidance for the interception of communication as follows:

- Include the legal definition of intercept to ensure that staff understand what constitutes a legal intercept;
- Clarify how 'reasonable grounds to believe' should be documented and supported to meet the rule of law;
- Clarify how and when authorization to intercept communication is to be provided to ensure CSC meets its legal obligations;
- Require that individuals with designated authority can authorize the interception of communication only after completing the NTS training, and signing an attestation;
- Clarify expectations for documenting intercept activity **(REDACTED)**;
- Clarify the manner in which inmates are to be notified that their communication has been intercepted and ensure that the notification form provides evidence that the notification took place;
- Establish direction for the retention, archiving onto DVD, and disposal of intercepted communication; and
- Set expectations for monitoring and reporting.

**Management Response**

The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By June 30, 2021 the ACCOP, supported by the Assistant Commissioner, Policy (ACP) will issue an interim policy bulletin clarifying direction related to the procedures for interception of communication and revise existing national policy on interception of communications to include, clarify and establish all of the suggested changes noted in Recommendation 1.

**Recommendation 2**

The Assistant Commissioner, Correctional Operations and Programs, in collaboration with the Assistant Commissioner, Corporate Services and the Assistant Commissioner, Human Resource Management, should ensure that the following training is provided:

- NTS continuous development training on the legal and policy framework for Security Intelligence Officers;
- NTS training on the legal and policy framework for Institutional Heads and Deputy Wardens; and
- Training on the voice logger.

**Management Response**

The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By March 31 2021, the ACCOP, in collaboration with the Assistant Commissioner, Human Resource Management (ACHRM), and the Assistant Commissioner, Corporate Services (ACCS) will: Identify training on the legal and policy framework as a National Training Standard for Security Intelligence Officers, Deputy Wardens, and Insitutional Heads; develop and ensure availability of training on the legal and policy framework for the interception of communication; and develop and ensure availability of training on the voice logger.

**Recommendation 3**

The Regional Deputy Commissioners should implement monitoring processes to ensure that:

- Reasonable grounds to believe is adequately documented and supported by reliable, credible and relevant intelligence information;
- Approval documentation is completed accurately and in its entirety;
- Authorizations are provided in writing, by an individual with designated authority, prior to intercepting communication; and
- Sharing of intelligence information is documented in accordance with CSC guidance.

**Management Response**

The Regional Deputy Commissioners (RDCs), the Assistant Commissioner, Correctional Operations and Programs (ACCOP) and the Assistant Commissioner, Policy (ACP) agree with this recommendation. By October 2020, the ACCOP in collaboration with the RDCs and the ACP will: Establish a process to monitor the reliability, credibility and relevance of authorizations to conduct interceptions, which will include ensuring the appropriate approvals are completed as required; and establish a process to monitor the appropriate and timely documentation of intelligence information.

## Recommendation 4

The Regional Deputy Commissioners should direct Institutional Heads to:

- Revise standing orders for the interception of communication to ensure that they are up-to-date, align with national guidance, and specify the rules and/or processes that are unique to their institution;
- Clarify in post orders the roles and responsibilities of staff in the visits and correspondence area for the interception of communication to ensure that their actions are aligned with legal requirements; and
- Implement rigorous quality assurance practices to ensure that:
    - All information entered into the voice logger, **(REDACTED)**, is complete, accurate, and up-to-date;
    - Communication is intercepted in accordance with authorizations;
    - Communication intercept activity is properly documented; and
    - Inmates are notified in a timely manner that their communication has been intercepted.

### Management Response

The Regional Deputy Commissioners (RDCs), the Assistant Commissioner, Correctional Operations and Programs (ACCOP) and the Assistant Commissioner, Policy (ACP) agree with this recommendation. By October 2020, the RDCs in collaboration with the ACCOP and the ACP will: Ensure standing orders for the interception of communication are updated; clarify in post orders the roles and responsibilities of staff in the visits and correspondence area for the interception of communication; and ensure quality assurance practices are implemented prior to intercepting communication.

## Recommendation 5

The Assistant Commissioner, Correctional Operations and Programs should:

- Define the level of access required for users of the voice logger; and
- Develop standards for the maintenance of user accounts on the voice logger.

### Management Response

The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By December 2019, the ACCOP, in collaboration with the Assistant Commissioner, Corporate Services (ACCS) will: Define the level of access required for users of the voice logger and Develop standards for the maintenance of user accounts on the voice logger.

**Recommendation 6**

The Assistant Commissioner, Correctional Operations and Programs, in coordination with the Assistant Commissioner, Policy should identify, analyze, and address privacy issues resulting from the interception of inmate communications to ensure compliance with applicable policy requirements.

**Management Response**

The Assistant Commissioner, Correctional Operations and Programs (ACCOP) agrees with this recommendation. By March 2021, the ACCOP, supported by the Assistant Commissioner, Policy (ACP), will ensure a process is in place to identify and effectively address any potential privacy issues arising out of the interception of inmate communications.

# 4.0 CONCLUSION

Overall, we found that elements of a management framework were in place; however, improvements were required to help ensure that the framework supported the efficient and effective achievement of communication intercept objectives. Through Phase 1, the audit noted that a lack of guidance and limited training caused institutional management and SIOs to have an incomplete understanding of the legal and policy requirements for intercepting inmate communications, which resulted in significant compliance issues. Specifically, reasonable grounds were often not adequately documented and/or supported by intelligence information, authorization to intercept an inmate's communication was not always provided in writing, and communication (including privileged) was intercepted without approval. These compliance issues went largely undetected due to insufficient quality assurance over the intercept work performed by the SIOs, and a lack of monitoring and reporting activity. We also identified that intercept activity was not always well-documented, and information obtained through intercept activity was not always properly managed. In addition, we found a lack of effective safeguards to ensure that CSC was meeting its legal and policy obligations with respect to notifying inmates that their communication has been intercepted.

Through Phase 2, we found that the immediate action taken by management resulted in significant improvements in compliance with key legislative and CSC policy requirements. We encourage CSC to continue to focus its efforts on the efficient and effective management and implementation of this important intelligence tool. Recommendations have been issued in the report based on areas where further improvements are required.

# 5.0 MANAGEMENT RESPONSE

Management agrees with the audit findings and recommendations as presented in the audit report. Management has prepared a detailed Management Action Plan to address the issues raised in the audit and associated recommendations. The Management Action Plan is scheduled for full implementation by June 30, 2021.

Upon completion of Phase 1, the Senior Deputy Commissioner in collaboration with the Assistant Commissioner Correctional Operations and Programs and the Regional Deputy Commissioners prepared an action plan to immediately address the most significant preliminary findings. The actions taken by management focused on the following three areas: providing training to institutional management and SIOs on the legal and policy framework as well as on the voice logger; implementing oversight and quality assurance processes at both RHQ and NHQ over authorizations to intercept; technical upgrades; and providing updated guidance to institutions. The following details the actions taken to date.

**Training**

In 2018, the Preventive Security and Intelligence (PSI) branch, in collaboration with CSC's Legal Services Unit (LSU), provided national refresher training on legislative principles and regulations for interception of communications as well as provided training on reasonable and probable grounds to Wardens, Deputy Wardens and Regional Intelligence Coordinators (RICs).

Training on the **(REDACTED)** were delivered nationally to all staff responsible for the administration of the **(REDACTED)**. The 2019 Security Intelligence Officer Continuous Development (SIOCD) training was developed to include an intercept gist-writing component and to include best practices and lessons learned from the audit results and ongoing national review of intercept gists.

Additionally, training for Deputy Wardens' and CSC's senior management outlining roles and responsibilities in relation to intelligence based policies and practices, was also developed, with particular focus on intercept related activities, development of reasonable grounds and management of privileged correspondence. This was presented as part of the Operational Senior Manager Interim Training Program.

**Oversight/ Accountability framework**

In an effort to introduce more robust oversight measures, a national review of intercepts gists between September 2018 and March 2019 was conducted. As of September 2019, the RICs started reviewing the interception of inmate communications authorization and notification forms to ensure adherence to applicable legislation and policies. Additionally, feedback from the ongoing national review of intercept gists are being provided to sites/SIOs upon request. In an effort to maintain consistency in the practical application of intercept activities, an intercept assessment reference tool for RHQ/NHQ staff was developed to support their quality assurance functions. A national intercept tracking mechanism (for RHQ/NHQ staff) is also being introduced, to monitor intercept activities and ensure the completion of adequate documentation in accordance with legislative and policy requirements. Further, a central database has been created at national headquarters for the electronic storage and retention of all intercept authorization requests and notifications to inmates of completed intercept activity, for better oversight and quality assurance purposes.

In June 2020, CSC Commissioner Anne Kelly approved the establishment of a National Intercept Centre at NHQ. This centre will assist in reducing corporate risks by increasing oversight of the intercept program and by leveraging intelligence information obtained from intercepted communications.

**Technical upgrades**

Between January and March 2019, CSC's Technical Services department in collaboration with **(REDACTED)** carried out national maintenance of all voice logger user accounts. In addition to system upgrades, **(REDACTED)** to enhance accountability and support better oversight at the site level.

PSI continues to collaborate with **(REDACTED)** to explore ways in which the **(REDACTED)** can be better utilised for operational purposes.

**Management direction to staff**

In response to the Internal Audit Sector's findings, summarising CSC's Interception of Inmate Communication practices, policies and identified areas for improvement, CSC's senior management provided national direction for the appropriate management of privileged correspondence. This direction also included operational guidance on the appropriate use of the **(REDACTED)**. Additionally, a memorandum was circulated to all regions identifying the applicable legislative regulations governing CSC's intercept program.

# 6.0 ABOUT THE AUDIT

## 6.1 Approach and Methodology

### 6.1.1 Phase 1

Audit evidence was gathered through a number of methods:

**Interviews:** were conducted with senior management and key staff at NHQ, RHQ and institutions selected for inclusion in Phase 1 of the audit. Interviews took place in person and by teleconference.

**Review of Documentation:** applicable legislation, CSC policy instruments, and corporate documents such as contracts, training manuals, institutional and staff reports, intelligence information contained in preventive security files, e-mails, institutional briefing materials, and information and records maintained in ITS and on the voice logger.

**Sampling Strategy and File Review**[40]**:** a non-statistical sample of files was selected for the period from January 1, 2017 to June 22, 2018. Files were selected starting with the most recent and working backwards in order to test those of greater relevance. File review was completed at each institution selected for inclusion in the audit and focused solely on intercepted telephone communication.

**Observations:** included the manner in which preventive security files are maintained, and the existence and operation of intercept equipment. Further, mail processes and inmate visits were observed to identify and assess the controls in place.

**Analytical Review:** was completed in relation to the criteria on guidance, training, equipment, monitoring and reporting, compliance with approval, and information security.

### 6.1.2 Phase 2

Audit evidence was gathered through a number of methods:

**Interviews:** were conducted with senior management and key staff at institutions selected for inclusion in Phase 2 of the audit. Interviews took place in person.

**Review of Documentation:** corporate documents such as training manuals, institutional and staff reports, intelligence information contained in preventive security files, and information and records maintained in ITS and on the voice logger.

**Sampling Strategy and File Review**[41]**:** a non-statistical sample of files was selected for the period from November 1, 2018 – April 12, 2019. Files were selected starting with the most recent and working backwards in order to test those of greater relevance. File review focused solely on intercepted telephone communication.

## 6.2 Past Audits and External Assurance Work

No CSC internal audit or external assurance work has been completed in the last five years that focused on the interception of inmate communications.

[40] For the purposes of the file review, one file is defined as an approval to intercept, including all extensions.
[41] ibid

## 6.3 Statement of Conformance

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The opinion is applicable only to the area examined.

The audit conforms to the Internal Auditing Standards for Government of Canada, as supported by the results of the quality assurance and improvement program. The evidence gathered was sufficient to provide senior management with proof of the opinion derived from the internal audit.

Christian D'Auray, CPA, CA

Chief Audit Executive

# ANNEX A: RESULTS OF COMPLIANCE TESTING

| Audit Test | Audit Result | |
|---|---|---|
| | Phase 1 | Phase 2 |
| Reasonable grounds were documented | **96% (80/83)** | **100% (62/62)** |
| Reasonable grounds were adequately documented | **60% (48/80)** | **79% (49/62)** |
| Reasonable grounds clearly referenced the supporting intelligence information | **38% (30/80)** | **81% (50/62)** |
| Intelligence information being referenced was documented | **73% (58/80)** | **86% (36/42)** |
| Approval was provided in writing | **96% (80/83)** | **98% (61/62)** |
| Approval was provided by an individual with appropriate authority | **100% (80/80)** | **N/A** |
| Approval was provided prior to start of the authorized intercept period | **93% (77/83)** | **94% (58/62)** |
| Initial intercepts were approved for a period of less than or equal to 30 days as required by CD 568-10 | **41% (32/79)** | **82% (51/62)** |
| Extensions were approved for a period of less than or equal to 15 days as required by CD 568-10 | **57% (16/28)** | **79% (11/14)** |
| Extensions were signed prior to the expiry of the authorization | **57% (16/28)** | **93% (13/14)** |
| Communications were intercepted within the authorized time period | **88% (68/77)** | **97% (60/62)** |
| Communications between an inmate and their lawyer were not intercepted | **90% (71/79)** | **95% (59/62)** |
| **(REDACTED)** were up-to-date | **0% (0/11)** | **18% (2/11)** |
| Recorded telephone calls were documented on form 1036 | **25% (20/79)** | **N/A** |
| Disposition of information obtained through telephone intercepts was documented on form 1036 | **13% (10/79)** | **N/A** |
| SIOs have their own user account on the voice logger (for sites visited) | **82% (18/22)** | **N/A** |
| **(REDACTED)** | **100% (9/9)** | **N/A** |
| Notification form was completed and on file | **88% (68/77)** | **N/A** |
| Inmate was notified of intercept activity | **Unable to assess** | **N/A** |

N/A – Test was not re-performed during Phase 2 of the audit.

# ANNEX B: AUDIT CRITERIA

The following table outlines the audit criteria developed to meet the stated audit objectives and audit scope.

| Audit Objective | Audit Criteria | Audit Result | |
|---|---|---|---|
| | | Phase 1 | Phase 2 |
| **Objective 1:** To provide assurance that the management framework in place supports the efficient and effective achievement of communication intercept objectives. | 1.1 Guidance - CSC guidance is complete, clear, and aligns with legislation. | Not met | N/A |
| | 1.2 Training - CSC provides training to support the discharge of responsibilities. | Not met | N/A |
| | 1.3 Equipment - CSC has in place the necessary equipment to intercept inmate communications. | Partially met | N/A |
| | 1.4 Monitoring - Monitoring is conducted on a regular basis and results are documented and reported to the required management level. | Not met | N/A |
| **Objective 2:** To provide assurance that key activities have been implemented in compliance with requirements. | 2.1 Reasonable grounds is adequately documented and supported by intelligence information. | Not met | Partially met |
| | 2.2 Approval to intercept is given in writing, by an individual with the appropriate authority, prior to the start of related intercept activity. | Not met | Met with exceptions |
| | 2.3 Interception is carried out in compliance with approvals. | Not met | Partially met |
| | 2.4 Information is appropriately secured and shared. | Not met | N/A |

N/A – Criterion was not reassessed during Phase 2 of the audit.

# ANNEX C: SITES VISITED

The following table indicates the sites that were selected for both Phases of the audit.

## Phase 1

The sites selected for Phase 1 were visited in May-June 2018. They were selected based on analysis of: volume of intercept activity (number of approvals to intercept), number of drug-related seizures (resulting from security intelligence information), rate of possess/transport drugs, rate of drug-related incidents, and rate of security incidents. In addition, travel constraints (i.e. time and resources) were taken into consideration when selecting the institutions.

## Phase 2

The sites selected for Phase 2 were visited in March-April 2019. They were selected based on analysis of: volume of intercept activity (number of approvals to intercept) during the scope period, and whether or not the site was included in Phase 1 of the audit. For the Pacific, Prairie, and Ontario regions, the audit team selected at least one site that was visited during Phase 1, and one that was not. Given that the Quebec and Atlantic regions were not visited during Phase 1, the sites for these regions were selected based on the volume of intercept activity during the scope period with consideration given to travel constraints (i.e. time and resources).

| Region | Sites Visited | |
|---|---|---|
| | Phase 1 | Phase 2 |
| **Atlantic** | Not visited | Atlantic Institution<br>Dorchester Penitentiary<br>Springhill Institution |
| **Quebec** | Not visited | Donnaconna Institution<br>Drummond Institution |
| **Ontario** | Millhaven Institution<br>Warkworth Institution<br>Collins Bay Institution<br>Beaver Creek Institution<br>Regional Headquarters | Millhaven Institution<br>Warkworth Institution<br>Bath Institution |
| **Prairie** | Drumheller Institution<br>Stony Mountain Institution<br>Bowden Institution<br>Regional Headquarters | Drumheller Institution<br>Edmonton Institution |
| **Pacific** | Matsqui Institution<br>Fraser Valley Institution for Women<br>Kent Institution<br>Mountain Institution<br>Regional Headquarters | Matsqui Institution<br>Mission Institution |
| **NHQ** | Various Sectors | Various Sectors |

# ANNEX D: CSC POLICY INSTRUMENTS

The following CSC policy instruments include requirements and processes that are related or applicable to the management of communication intercepts.

- CD 085 Correspondence and Telephone Communication
- CD 225 Information Technology Security
- CD 340 Electronic Security Systems
- CD 568 Management of Security Information and Intelligence
- CD 568-2 Recording and Sharing of Security Information and Intelligence
- CD 568-4 Preservation of Crime Scenes and Evidence
- CD 568-10 Interception of Inmate Communications
- GL 005-1 Institutional Management Structure: Roles and Responsibilities
- GL 340-1 Electronic Security System Scope
- Institutional Standing Orders

# ANNEX E: PRIVILEGED COMMUNICATION

Pursuant to the CCRR, communication between an inmate and the following individuals is considered privileged communication and cannot be legally intercepted unless specific legislative requirements have been met.

1. Governor General of Canada
2. Solicitor General of Canada
3. Judges and provincial court judges of Canadian courts, including the registrars of those courts
4. Members of the Senate
5. Members of the House of Commons
6. Consular officials
7. Members of provincial legislatures
8. Members of the Legislative Council for the Yukon or the Northwest Territories
9. Deputy Solicitor General of Canada
10. Commissioner of the Correctional Service of Canada
11. Chairperson of the National Parole Board
12. Commissioner of Official Languages
13. Canadian Human Rights Commission
14. Information Commissioner
15. Privacy Commissioner
16. Provincial ombudspersons
17. Assistant Commissioner, Audit and Investigations of the Correctional Service of Canada
18. Privacy Co-ordinators of federal departments
19. Correctional Investigator of Canada
20. Legal counsel

# ANNEX F: APPLICABLE CSC FORMS

The following is a list of CSC forms that are utilized during the interception of an inmate's communication.

1. Express Consent to Intercept a Private Conversation (CSC form 1453)
2. Authorization to Intercept Inmate Communications (CSC form 1454)
3. Record of Intercepted Communications (CSC form 1036)
4. Notice of Interception of Communications and Correspondence (CSC form 1135)
5. Security Intelligence Report (CSC form 0232)
6. Intelligence Observation Report (CSC form 1445)
7. Security Intelligence Briefing Record (CSC form 1443)
8. Partner Liaison Log (CSC form 1442)

# ADDENDUM A: FOLLOW-UP RESULTS

In October 2019, the Internal Audit Sector was asked to conduct follow-up work to assess if actions taken to address issues identified during Phases 1 and 2 of the audit led to improved compliance. Site visits for this follow-up work was completed in February and March, 2020, and included visits to 20 institutions across all five regions. Compliance testing was completed for a sample of communication intercepts that were internally authorized between November 1, 2019 and February 21, 2020.

| Audit Test | Audit Result |
|---|---|
| Reasonable grounds were documented | **100% (72/72)** |
| Reasonable grounds were adequately documented | **86% (62/72)** |
| Reasonable grounds clearly referenced the supporting intelligence information | **89% (64/72)** |
| Intelligence information being referenced was documented | **88% (63/72)** |
| Approval was provided in writing | **100% (72/72)** |
| Approval was provided prior to start of the authorized intercept period | **99% (71/72)** |
| Initial intercepts were approved for a period of less than or equal to 30 days as required by CD 568-10 | **85% (61/72)** |
| Extensions were approved for a period of less than or equal to 15 days as required by CD 568-10 | **71% (10/14)** |
| Extensions were signed prior to the expiry of the authorization | **93% (13/14)** |
| Communications were intercepted within the authorized time period | **98% (54/55)** |
| Communications between an inmate and their lawyer were not intercepted | **95% (52/55)** |
| **(REDACTED)** were up-to-date | **15% (3/20)** |
| **(REDACTED)** | **30% (6/20)** |

**Sites visited**

| Region | Sites Visited |
|---|---|
| **Atlantic** | Atlantic Institution<br>Dorchester Penitentiary |
| **Quebec** | Drummond Institution<br>Donnaconna Institution<br>Federal Training Center |
| **Ontario** | Bath Institution<br>Beaver Creek Institution<br>Collins Bay Institution<br>Joyceville Institution<br>Millhaven Institution<br>Warkworth Institution |
| **Prairie** | Bowden Institution<br>Edmonton Institution<br>Saskatchewan Penitentiary<br>Stony Mountain Institution |
| **Pacific** | Kent Institution<br>Matsqui Institution<br>Mission Institution<br>Mountain Institution<br>Pacific Institution |